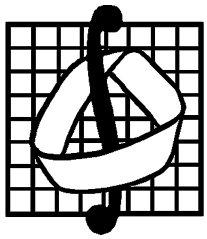
МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
имени М. В. ЛОМОНОСОВА



МЕХАНИКО-МАТЕМАТИЧЕСКИЙ ФАКУЛЬТЕТ

МАТЕРИАЛЫ

X Международного семинара

«ДИСКРЕТНАЯ МАТЕМАТИКА И ЕЕ ПРИЛОЖЕНИЯ»

(Москва, 1–6 февраля 2010 г.)

Издательство механико-математического факультета МГУ

Москва 2010

М34
УДК 519.7

Издание осуществлено при поддержке Российского фонда фундаментальных исследований по проекту 10–01–06004–г

М34 Материалы X Международного семинара «Дискретная математика и ее приложения»(Москва, МГУ, 1–6 февраля 2010 г.) / Под редакцией О. М. Касим-Заде. — М.: Изд-во механико-математического факультета МГУ, 2010. — 549 с.

Сборник содержит материалы X Международного семинара «Дискретная математика и ее приложения», проходившего на механико-математическом факультете МГУ имени М. В. Ломоносова с 1 по 6 февраля 2010 г. при поддержке Российского фонда фундаментальных исследований (проект 10–01–06004). Для студентов, аспирантов и научных работников в области дискретной математики и математической кибернетики.

Научное издание

МАТЕРИАЛЫ
X МЕЖДУНАРОДНОГО СЕМИНАРА
«ДИСКРЕТНАЯ МАТЕМАТИКА И ЕЕ ПРИЛОЖЕНИЯ»
(Москва, МГУ, 1–6 февраля 2010 г.)

Под общей редакцией О. М. КАСИМ-ЗАДЕ

Редакционная группа:
К. А. Зыков, Р. М. Колпаков, В. В. Кочергин, А. В. Чашкин

Ответственный за выпуск *В. В. Кочергин*

Н/К
ИД № 04059 от 20.02.2001 Подписано к печати 10.03.2010. Формат 60 × 90/16.
Бумага типогр. № 1. Печ. л. 34,5. Тираж 300 экз.
Издательство механико-математического факультета МГУ. 119991, Москва, Ленинские горы, МГУ.
Отпечатано с оригинал-макета в типографии ООО «Гипрософт», Москва

© Коллектив авторов, 2010

ПРЕДИСЛОВИЕ

X Международный семинар «Дискретная математика и ее приложения» проходил на механико-математическом факультете МГУ имени М. В. Ломоносова с 1 по 6 февраля 2010 г. при поддержке Российского фонда фундаментальных исследований (проект 10–01–06004–г).

Оргкомитетом семинара до начала его работы были разосланы информационные письма в ведущие научные центры и университеты стран СНГ, отобраны наиболее интересные доклады и сообщения для заслушивания на пленарных и секционных заседаниях.

Семинар собрал более 250 участников (в том числе более 60 докторов наук) из 40 научных центров России, Беларуси, Украины, Молдовы и Азербайджана.

Работа семинара проходила в шести секциях:

— синтез, сложность и надежность управляющих систем,

— теория функциональных систем,

— комбинаторный анализ и теория графов,
подсекции:
  — комбинаторный анализ,
  — теория графов,

— математическая теория интеллектуальных систем,

— дискретная геометрия,

— теория кодирования и математические воросы теории защиты информации

Всего было заслушано 18 пленарных и 194 секционных доклада; содержание большинства из них отражено в настоящем сборнике.

Тексты публикуются в авторской редакции (исправлены замеченные опечатки).

ПЛЕНАРНЫЕ ДОКЛАДЫ

ОБ АРИФМЕТИЧЕСКИХ ПОДХОДАХ К ЗАДАЧАМ КРИПТОГРАФИИ

М. П. Минеев, В. Н. Чубариков (Москва)

1. Введение

Наиболее простой тип преобразования исходного текста состоит в том, что происходит замена каждой буквы алфавита некоторой буквой с помощью подстановки этого алфавита. Такой шифр называется шифром простой однобуквенной замены.

Метод вскрытия шифра простой замены использует частотные характеристики появления фиксированной буквы или сочетания букв первоначального открытого текста, которые совпадают с частотными характеристиками зашифрованного текста. Подтверждением устойчивости этой характеристики служит закон больших чисел, согласно которому частота появления любой фиксированной буквы в достаточно длинном тексте при дополнительной гипотезе о независимости появления каждой буквы практически одна и та же на протяжении всего текста. Опыт показывает, что с определенной точностью этот закон справедлив для реальных открытых текстов (например, текстов литературных произведений прозы). Имеются таблицы частот появления букв в разнообразных текстах различных языков мира.

Первое, дошедшее до нас, описание подобного частотного метода криптоанализа относится к IX веку [1, с. 30–32]. Оно принадлежит известному "философу арабского мира" Абу Юсуф Якуб ибн Исхак ибн ас-Сабах ибн Умран ибн Исмаил аль-Кинди. Его знаменитый трактат "Рукопись по дешифрованию криптографических сообщений" был открыт в 1987 г. в Стамбуле в оттоманском архиве Сулаймaнийа. Как указывает С. Сингх [1], в этом трактате дан подробный анализ статистики, фонетики и синтаксиса арабского языка и приведена "революционная система криптоанализа" аль-Кинди, которая умещается в следующие два коротких абзаца.

"Один из способов прочесть зашифрованное сообщение, если мы знаем язык, на котором оно написано, это взять другой незашифрованный текст на том же языке, размером на страницу или около того, и затем подсчитать появление в нем каждой из букв. Назовем наиболее часто встречающуюся букву "первой", букву, которая

по частоте появления стоит на втором месте, назовем “вторая”, букву, которая по частоте появления стоит на третьем месте, назовем “третья” и т. д., пока не будут сочтены все различные буквы в незашифрованном тексте.

Затем посмотрим на зашифрованный текст, который мы хотим прочитать, и таким же способом проведем сортировку его символов. Найдем наиболее часто встречающийся символ и заменим его “первой” буквой незашифрованного текста, второй по частоте появления символ заменим “второй” буквой, третий по частоте появления символ заменим “третьей” буквой и т. д., пока не будут заменены все символы зашифрованного сообщения, которое мы хотим дешифровать.”

Следует отметить, что и сам криптоанализ аль-Кинди мог появиться в то время только при достижении достаточно высокого уровня развития как светского образования в таких науках, как математика, статистика и лингвистика, так и религиозного образования.

Для того, чтобы значительно усложнить задачу вскрытия шифра простой замены применяют методы “рандомизации” и “сжатия” открытых текстов [2, с. 106]. Они используются в компьютерных архиваторах.

Другой пример “сжатия” текста приводится в книге С. Сингха [1, прил. F, с. 416–417]: “Шифр ADFGVX”.

Зашифровывание здесь состоит в том, матрица размером 6×6 заполняется 26 буквами и 10 цифрами в произвольном порядке. Каждая строка и каждый столбец задаются одной из шести букв: A, D, F, G, V и X. Расположение элементов в матрице служит ключом. Например, матрица имеет вид

	A	D	F	G	V	X
A	8	p	3	d	1	n
D	l	t	4	o	a	h
F	7	k	b	c	5	z
G	j	u	6	w	g	m
V	x	s	v	i	r	2
X	9	e	y	0	f	q

Каждый символ в матрице зашифровывается буквами, которые обозначают строку и столбец, в котором находится этот символ. Например, “8” заменяется на “AA”, символ “p” — на “AD”.

Таким образом шифртекст будет использовать только 6 букв: A, D, F, G, V, X. Тем самым, произведено “сжатие” алфавита, но тем не менее для взлома шифрсообщения здесь достаточно воспользоваться частотным анализом для биграмм. Как указано в [1], применение дополнительно перестановки символов с использованием еще одного

ключа приводит к более сложному криптоанализу. Буквы A, D, F, G, V, X выбраны с той целью, чтобы они существенно отличались в представлении в виде точек и тире азбуки Морзе.

Отметим также, что указанные выше виды шифрования основаны на комбинаторных соображениях.

Здесь предлагается другой подход прямого искажения частот появления знаков в шифрованном тексте, основанный на арифметических функциях извлечения корня квадратного и возведения в квадрат чисел по некоторому модулю.

2. Метод искажения знаков в шифре простой замены с помощью извлечения корня квадратного

Изложим метод искажения знаков в шифре простой замены с помощью извлечения корня квадратного по некоторому модулю. Пусть алфавит открытого текста состоит из n букв. Шифрование исходного текста способом простой однобуквенной замены [3–13] основано на некоторой подстановке множества букв алфавита. Следовательно, эта подстановка является ключом такой криптосистемы, и, значит, количество возможных ключей будет равно $n!$. Отметим, что различным символам шифрованного текста соответствуют различные буквы. В исходном тексте различные буквы, как правило, встречаются с разной частотой.

В качестве модельной ситуации рассмотрим русский алфавит, состоящий из 31 буквы (отождествляются буквы е,ё и ь,ъ). Известна таблица относительных частот встречаемости букв этого алфавита, упорядоченная в порядке убывания частот, в тексте на русском языке (см., например, [12]). Расположим буквы в порядке убывания частот:

1) о — 0,090, 2) е, ё — 0,072, 3) а — 0,062, 4) и — 0,062, 5) н — 0,053, 6) т — 0,053, 7) с — 0,045, ..., 31) ф — 0,002.

Поскольку число 31 — простое, все вычеты по модулю 31 можно разбить на три класса: квадратичные вычеты, квадратичные невычеты и вычет, отвечающий нулю. Как известно, количество квадратичных невычетов и количество квадратичных вычетов в полной системе вычетов по простому модулю одинаково и в данном случае оно равно 15. Все квадратичные вычеты по модулю 31 исчерпываются следующими классами вычетов по модулю 31: $1, 2^2, 3^2, \ldots, 15^2$. Занумеруем сначала все наименьшие положительные квадратичные вычеты по модулю 31 по убыванию их величины, а затем также занумеруем квадратичные невычеты в порядке убывания.

Если a — квадратичный вычет по модулю 31, то решения сравнения $x^2 \equiv a \pmod{31}$ представляют собой два различных вычета по модулю 31: $a_1 = b$ и $a_2 = 31 - b$.

Рассмотрим теперь некоторый открытый текст и зашифруем его

с помощью метода простой замены. Расположим буквы шифрованного текста в порядке убывания частот, нумеруя их от 1 до 31.

Каждой из первых пятнадцати занумерованных букв взаимно однозначно сопоставим квадратичные вычеты по модулю 31 в соответствии с их порядком нумерации, затем следующие пятнадцать букв взаимно однозначно отобразим в квадратичные невычеты по модулю 31 также в соответствии с их порядком нумерации и, наконец, оставшейся букве сопоставим нулевой вычет по модулю 31.

Далее продолжим шифрование следующим образом. Пусть буква α зашифрована числом a и a — квадратичный вычет по модулю 31, и пусть вычеты a_1, a_2 решения сравнения $x^2 \equiv a \pmod{31}$. Тогда последовательности указанного числа a в криптограмме шифра простой замены ставим в соответствие последовательность чисел $a_1, a_2, a_1, a_2, \ldots$. Например, если в криптограмме имеется 5 мест, на которых стоит число a, то заменяем в этих местах число a на следующую последовательность чисел a_1, a_2, a_1, a_2, a_1. Пусть, теперь, буква α закодирована числом a и a — квадратичный невычет по модулю 31 или 0. Тогда в криптограмме это число a оставляем без изменения.

Для восстановления первоначальной криптограммы надо все числа, отвечающие квадратичным вычетам по модулю 31 возвести в квадрат по модулю 31.

Остается передать получателю текста номера тех мест, на которых стоят квадратичные невычеты по модулю 31. Осуществим это следующим образом.

Последовательно обозначим места, на которых стоят квадратичные вычеты по модулю 31, — единицами, а места, на которых стоят квадратичные невычеты, — нулями. Полученную последовательность чисел $\varepsilon_1, \ldots, \varepsilon_n$, составленную из нулей и единиц, можно рассматривать как запись некоторого числа m в двоичной системе счисления. Таким образом отправителю достаточно передать построенное число m.

Итак, абонент $\mathcal{A}$ должен послать "секретное" число m абоненту $\mathcal{B}$ по каналу связи.

Для этого можно воспользоваться, например, известным алгоритмом А. Шамира для передачи секретной информации по каналу связи (см., например, [11, 12, 16]). Приведем здесь этот алгоритм.

Абоненты $\mathcal{A}$ и $\mathcal{B}$ выбирают достаточно большое простое число $p > m$. Затем абонент $\mathcal{A}$ выбирает секретный ключ a, $1 < a < p - 1$, $(a, p-1) = 1$, а абонент $\mathcal{B}$ — секретный ключ b, $1 < b < p-1$, $(b, p-1) = 1$. Для проверки условия взаимной простоты a и $p-1$ абонент $\mathcal{A}$ может использовать алгоритм Евклида. В случае, если числа a и $p-1$ не взаимно просты, следует проверить на взаимную простоту числа $a+1$ и $p-1$ и т. д. Указанный процесс выбора ключа a оборвется

через конечное число шагов, так как, например, $(p-2, p-1) = 1$. Аналогичным образом может поступить и абонент $\mathcal{B}$. Далее абонент $\mathcal{A}$ находит натуральное число α такое, что

$$a\alpha \equiv 1 \pmod{p-1},\ 1 < \alpha < p-1.$$

Аналогично поступает абонент $\mathcal{B}$. Он находит число β с условиями

$$b\beta \equiv 1 \pmod{p-1},\ 1 < \beta < p-1.$$

Итак, абонент $\mathcal{A}$ имеет секретный ключ (a, α), а абонент $\mathcal{B}$ — секретный ключ (b, β).

Теперь абонент $\mathcal{A}$ пересылает число m абоненту $\mathcal{B}$ по открытому каналу за следующие четыре шага.

1-й шаг. Абонент $\mathcal{A}$ посылает абоненту $\mathcal{B}$ число

$$m_1 \equiv m^a \pmod{p},\ 0 < m_1 < p-1.$$

2-й шаг. Абонент $\mathcal{B}$ посылает абоненту $\mathcal{A}$ число

$$m_2 \equiv m_1^b \pmod{p},\ 0 < m_2 < p-1.$$

3-й шаг. Абонент $\mathcal{A}$ посылает абоненту $\mathcal{B}$ число

$$m_3 \equiv m_2^\alpha \pmod{p},\ 0 < m_3 < p-1.$$

4-й шаг. Абонент $\mathcal{B}$ находит число m с помощью секретного ключа β следующим образом:

$$m = m_4 \equiv m_3^\beta \pmod{p},\ 0 < m_4 < p-1.$$

Действительно, имеем

$$m_4 \equiv m^{ab\alpha\beta} = m^{a\alpha \cdot b\beta} \equiv m \pmod{p},$$

т. е. получаем $m_4 \equiv m \pmod{p},\ 0 < m,\ m_4 < p-1$.

Следовательно, $m = m_4$.

Далее можно рекуррентным образом продолжить процедуру "сжатия алфавита".

Пусть l — натуральное число и q — простое число вида $q = 2^l + 1$. Тогда простое число q обязано быть простым числом Ферма $q = F_m = 2^{2^m} + 1, m \geq 0$. На сегодняшний день известно только пять простых чисел Ферма $F_0 = 3, F_1 = 5, F_2 = 17, F_3 = 2^8 + 1 = 257$ и

$F_4 = 2^{16} + 1 = 65537$. Мультипликативная группа поля F_q является циклической и состоит из $q-1 = 2^l$ элементов. Каждый из них имеет порядок $2^k, 0 \leq k \leq 2^l$.

Пусть теперь алфавит A состоит из $q = 2^l + 1, l = 2^m, 0 \leq m \leq 4$, символов. Тогда, используя процедуру, описанную выше, в точности l раз, приходим к шифрованному тексту, алфавит которого отвечает только квадратичным невычетам и нулевому вычету по модулю q. Таким образом алфавит шифрованного текста будет состоять из $(q+1)/2$ символа.

3. Метод искажения знаков в шифре простой замены с помощью возведения в квадрат

Дадим способ искажения частот встречаемости букв в шифртексте, получаемого простой заменой и основанного на арифметической функции возведения в квадрат по некоторому модулю.

Опишем процедуру шифрования.

Пусть, как и раньше, алфавит сообщения состоит из 31 буквы (например, русский алфавит, в котором отождествляются буквы е, ё и ь, ъ). Расположим буквы этого алфавита в порядке убывания частот их появления в открытом тексте.

Разобьем все вычеты по модулю 31 на два класса: первый класс состоит из 15 квадратичных невычетов, второй — из 15 квадратичных вычетов и нуля.

1. Зашифруем открытый текст методом простой замены с помощью некоторой подстановки.

2. Расположим буквы шифрованного текста в порядке убывания частот. После этого каждой из первых пятнадцати букв присвоим последовательные значения квадратичных невычетов по модулю 31 в соответствии с их порядком нумерации, затем остальным буквам присваиваются последовательные значения квадратичных вычетов и 0.

3. Далее, тем буквам зашифрованного текста в соответствии с пунктом 2, которым соответствуют квадратичные невычеты поставим в соответствие квадраты этих чисел по модулю 31 из отрезка $[0, 30]$, а для букв, отвечающих квадратичным вычетам и нулю, сохраним те же значения квадратичных вычетов и нуля.

4. Подведем итог процедуры шифрования. Итак, получен зашифрованный текст S, алфавит которого состоит только из квадратичных вычетов и нуля по модулю 31, т. е. содержит только 16 знаков.

5. Чтобы провести расшифрование, надо знать те места, на которых стоят квадраты квадратичных невычетов. Для этого составим двоичное число m, отвечающее шифртексту, следующим образом: те места, на которых стояли квадратичные невычеты, обозначим 1, а остальные — 0.

Тем самым, процедура шифрования завершена.

Процедура расшифрования происходит следующим образом.

А. Абоненту передается зашифрованный текст S и число m. Число m передается с помощью алгоритма А. Шамира.

Б. Для восстановления первоначальной криптограммы, полученной в пункте 1, необходимо на местах, отвечающих 1 в двоичной записи числа m (т. е. на местах, где стоят квадраты квадратичных невычетов), поставить первоначальные квадратичные невычеты, решая сравнение $x^2 \equiv t \pmod{31}$ относительно x, причем надо выбрать именно то решение данного сравнения, которое возводилось в квадрат.

В. При простом числе $p = 31$ имеем $p \equiv 3 \pmod 4$. Тогда вычет числа -1 является квадратичным невычетом по модулю 31. Пусть a — квадратичный невычет по модулю 31. Тогда сравнению $x^2 \equiv a^2 \pmod{31}$ отвечают два решения a и $-a \pmod{31}$, из которых a — квадратичный невычет (по выбору), и $-a = (-1)a$ является квадратичным вычетом, как произведение двух квадратичных невычетов.

Г. Простой способ извлечения корня квадратного из числа b простому модулю $p \equiv 3 \pmod 4$ (см., например, [14]), т. е. способ нахождения решения сравнения $x^2 \equiv b \pmod p$, таков: $x \equiv \pm b^{\frac{p+1}{2}} \pmod p$. Проверка числа на принадлежность к квадратичным вычетам или невычетам по модулю p осуществляется с помощью критерия Л. Эйлера: $\left(\frac{x}{p}\right) \equiv x^{\frac{p-1}{2}} \pmod p$.

Пусть, теперь, количество букв алфавита будет простым числом p, сравнимым с 1 по модулю 4. Разобьем все вычеты по модулю p на два класса: в первый класс войдут все квадратичные невычеты по модулю p, не превосходящие $(p-1)/2$ (их количество равно $(p-1)/4$); во второй класс — оставшиеся квадратичные невычеты, все квадратичные вычеты и 0.

Процедура шифрования по сравнению с предыдущей несколько модифицируется.

1. Как и раньше, текст шифруется способом простой замены.

2. Затем буквы шифрованного текста располагаем в порядке убывания частот их появления. Первым $(p-1)/4$ буквам присваиваем значения последовательных квадратичных невычетов из первого класса, остальным буквам присваиваем значения из второго класса.

3. Буквам, которые соответствуют числа из первого класса, поставим в соответствие квадраты этих чисел по модулю p из отрезка $[0, p-1]$.

4. Составим двоичное число m, отвечающее шифртексту, следующим образом: места, на которых находятся числа из первого класса, обозначим 1, а остальные — 0.

Далее поступаем, как в предыдущем случае. Отметим, что извлечение квадратного корня по модулю p в данном случае будет несколько сложнее [14].

4. Комбинированный метод искажения частот появления знаков в шифре простой замены

Опишем комбинированный метод искажения частот появления знаков в шифре простой замены, основанный на предыдущих методах возведения в квадрат и извлечения корня квадратного по некоторому модулю. Пусть, как и прежде, алфавит состоит из 31 знака.

1. Возьмем любую подстановку из 31 знака и зашифруем текст методом простой замены с помощью этой подстановки.

2. Расположим буквы шифрованного текста в порядке убывания частот. После этого каждой из первых пятнадцати букв присвоим последовательные значения квадратичных невычетов по модулю 31 в соответствии с их порядком нумерации, затем остальным буквам присваиваются последовательные значения квадратичных вычетов и 0.

3. Далее, тем буквам зашифрованного текста в соответствии с пунктом 2, которым соответствуют квадратичные невычеты поставим в соответствие квадраты этих чисел по модулю 31 из отрезка $[0, 30]$, а для букв, отвечающих квадратичным вычетам и нулю, поставим в соответствие значения квадратных корней из этих вычетов по модулю 31 и нуля, причем для квадратичного вычета a по модулю 31 решения $a_1, a_2, (a_1 < a_2)$ сравнения $x^2 \equiv a \pmod{31}$ заменяют последовательность чисел a в криптограмме на последовательность чисел $a_1, a_2, a_1, a_2, \ldots$.

4. Наконец, составим двоичное число m, отвечающее шифртексту, следующим образом: те места, на которых стояли квадратичные невычеты, обозначим 1, а остальные — 0.

Процедура шифрования завершена.

Опишем процедуру расшифрования.

А. Абоненту передается зашифрованный текст S и число m. Число m передается с помощью алгоритма А. Шамира.

Б. Для восстановления первоначальной криптограммы, полученной в пункте 1, необходимо на местах, отвечающих 1 в двоичной записи числа m (т. е. на местах, где стоят квадраты квадратичных невычетов), поставить первоначальные квадратичные невычеты, решая сравнение $x^2 \equiv t \pmod{31}$ относительно x, причем надо выбрать именно то значение x, которое возводилось в квадрат.

При простом числе $p = 31$ имеем $p \equiv 3 \pmod{4}$. Тогда вычет числа -1 является квадратичным невычетом по модулю 31. Пусть a — квадратичный невычет по модулю 31. Тогда сравнению $x^2 \equiv a^2 \pmod{31}$ отвечают два решения a и $-a \pmod{31}$, из которых a —

квадратичный невычет (по выбору), и $-a = (-1)a$ является квадратичным вычетом, как произведение двух квадратичных невычетов.

Способ извлечения корня квадратного из числа b по простому модулю $p \equiv 3 \pmod 4$, т. е. нахождения решения сравнения $x^2 \equiv b \pmod p$, дается соотношением $x \equiv \pm b^{\frac{p+1}{2}} \pmod p$. Проверка числа на принадлежность к квадратичным вычетам или невычетам по модулю p осуществляется с помощью критерия Л. Эйлера: $\left(\frac{x}{p}\right) \equiv x^{\frac{p-1}{2}} \pmod p$.

В. Продолжим восстановление первоначальной криптограммы. На местах, отвечающих 0 в двоичной записи числа m, поставим первоначальные значения квадратичных вычетов по модулю 31, возводя в квадрат вычеты, стоящие на этих местах.

Процедура расшифрования завершена.

5. Анализ методов искажения знаков в шифре простой замены

Возможности, связанные с использованием шифра простой замены с дальнейшим сглаживанием частот появления знаков в зашифрованном тексте, требуют установления степени сглаживания. Здесь можно пойти по следующему пути.

В шифре простой замены соответствующие частоты появления знаков в зашифрованном тексте и в первоначальном открытом тексте совпадают. Поэтому возникает задача о “сглаживании” и “искажении” этих частот, в частности, о приближении ее к равномерному распределению частот появления знаков в шифрованном тексте или о замене априорной функции распределения появления частот алфавитных символов открытого текста другой функцией распределения их частот в зашифрованном тексте.

При анализе зашифрованного текста можно выделить характерные черты последовательности действий.

1. Установление количества различных алфавитных символов в зашифрованном тексте.

2. Подсчет частот появления алфавитных символов и определенных сочетаний этих символов в зашифрованном тексте.

3. Нахождение особенностей зашифрованного текста: распознавание алфавитных символов, отвечающих гласным и согласным буквам в открытом тексте; выявление наиболее распространенных сочетаний символов и т. п.

Пусть количество различных алфавитных символов $a_1, \ldots, a_n$ зашифрованного текста равно n, а сам зашифрованный текст состоит из N алфавитных символов. Символами $N_k, N_{l,m}$ обозначим количество появлений в зашифрованном тексте символа $a_k, k = 1, \ldots, n$ и соответственно наборов символов $(a_l, a_m), l, m = 1, \ldots, n$. Количе-

ство всех возможных различных наборов (a_l, a_m) обозначим через b. Тогда имеем $b \le n^2$. Пусть $d_k = \frac{N_k}{N}$ — частота появления символа a_k, а величина $b_{l,m} = \frac{N_{l,m}}{N}$ — частота появления набора (a_k, a_l).

Как известно, в шифре простой замены ключ шифрования определяется подстановкой σ символов алфавита открытого текста.

Определим характеристики приближения к равномерному распределению при всех возможных шифрах простой замены данного открытого текста следующим образом

$$M = \min_{\sigma} \sum_{k=1}^{n} \left| d_k - \frac{1}{n} \right|, B = \min_{\sigma} \sum_{l,m=1}^{n} \left| b_{l,m} - \frac{1}{b} \right|.$$

Равномерность распределения алфавитных символов зашифрованного сообщения можно охарактеризовать также в духе критерия Г. Вейля равномерного распределения последовательности по модулю единица. Пусть $1 \le s_{k,1} < s_{k,2} < \cdots \le N$ и $1 \le t_{l,m,1} < t_{l,m,2} < \ldots$ — номера, которые занимает буква a_k, $k = 1, \ldots, n$, и соответственно набор (a_l, a_m) в зашифрованном тексте с помощью шифра простой замены, отвечающего подстановке σ. Рассмотрим при любом фиксированном целом $h \ne 0$ суммы

$$S_k(\sigma) = \frac{1}{N_k} \sum_{s_{k,l} \le N} e^{2\pi i h \frac{s_{k,l}}{n}}, \quad T_{l,m}(\sigma) = \frac{1}{N_{l,m}} \sum_{\substack{r \\ t_{l,m,r} \le N}} e^{2\pi i \frac{t_{l,m,r}}{n}}.$$

Тогда величина W, определяемая соотношением

$$W = \min_{\sigma} \sum_{k=1}^{n} |S_k(\sigma)|, \quad D = \min_{\sigma} \sum_{l,m=1}^{n} |T_{l,m}|,$$

будет характеризовать открытый текст и равномерность появления знаков в шифре простой замены.

6. Применение китайской теоремы об остатках к шифру Виженера

Продолжим построение шифров на основе теоретико-числовых алгоритмов [3–5].

Рассмотрим известный многоалфавитный шифр Виженера. Он является обобщением одноалфавитного шифра простой замены и шифром гаммирования с периодической гаммой (см., например, [7, с. 151–152; 8, с. 11]).

Пусть количество символов алфавита равно составному числу n. Каждому символу α_r, $r = 1, \ldots, n$, алфавита присваивается некоторый вычет a_r по модулю n, причем различным символам отвечают различные вычеты. Пусть, также, число n представимо в виде $n = dq, (d, q) = 1, d > 1, q > 1$. Например, $n = 35 = dq = 5 \cdot 7$ или $n = 36 = 4 \cdot 9$.

Тогда можно предложить следующий способ шифрования.

1. *Предварительные преобразования.* Представим каждое число $1 \leq a \leq n$ в виде

$$a \equiv qb + dc \pmod{n}, \tag{1}$$

где $1 \leq b \leq d, 1 \leq c \leq q$. Тогда по китайской теореме об остатках вычет a по модулю n однозначно определяет вычеты b по модулю d и c по модулю q и наоборот.

Составим две таблицы Виженера, отвечающие вычетам b и c. Пусть $b_1, \ldots, b_d$ — полная система вычетов по модулю d, например, $1, 2, \ldots, d$, и $c_1, \ldots, c_q$ — полная система вычетов по модулю q. Тогда таблицы Виженера будут иметь вид

$$\begin{array}{ll} \underline{b_1, b_2, \ldots, b_{d-1}, b_d,} & \underline{c_1, c_2, \ldots, c_{q-1}, c_q,} \\ b_2, b_3, \ldots, b_d, \quad b_1, & c_2, c_3, \ldots, c_q, \quad c_1, \\ \ldots\ldots\ldots\ldots\ldots & \ldots\ldots\ldots\ldots\ldots \\ b_d, b_1, \ldots, b_{d-2}, b_{d-1}, & c_q, c_1, \ldots, c_{q-2}, c_{q-1}. \end{array}$$

Для каждой из приведенных выше таблиц Виженера при некоторых натуральных числах s, t с условиями $1 \leq s \leq d, 1 \leq t \leq q$, возьмем свой ключ $k = (b_{k_1}, b_{k_2}, \ldots, b_{k_s})$ для первой таблицы и соответственно $p = (c_{p_1}, c_{p_2}, \ldots, c_{p_t})$ для второй таблицы. Над каждым вычетом первой строки первой таблицы выписываем в строку символы ключа k следующим образом

$$b_{k_1}, b_{k_2}, \ldots b_{k_s}, b_{k_1}, b_{k_2}, \ldots.$$

Аналогично выписываем ключ p над второй таблицей.

2. *Процедура шифрования открытого текста.*

Пусть задан открытый текст $a_{h_1} a_{h_2} \ldots a_{h_u}$. По формуле (1) преобразуем его в два текста. Имеем

$$b_{h_1} b_{h_2} \ldots b_{h_u}; \quad c_{h_1} c_{h_2} \ldots c_{h_u}.$$

На пересечении h_1-го столбца и k_1-й строки в первой таблице находим символ x_1, а на пересечении h_1-го столбца и p_1-й строки

второй таблицы находим символ y_1. Повторим эту процедуру для следующего символа a_{h_2} и т. д. Получим шифрованный текст

$$x_1y_1x_2y_2\dots x_uy_u$$

или два шифрованных текста $x_1x_2\dots x_u$ и $y_1y_2\dots y_u$, или $z_1z_2\dots z_u$, где $z_t = qx_t + dy_t, 1 \le t \le u$.

3. *Процедура расшифрования.*

По ключам k и p в первой и второй таблицах Вижинера находим строки с номерами k_1 и p_1 соответственно. На этих строках находим элементы x_1 в первой таблице и y_1 во второй таблице, а затем по этим элементам находим, отвечающие им столбцы, и получаем элементы b_{h_1} и c_{h_1}. По тому же правилу восстанавливаются элементы b_{h_2} и c_{h_2} и т. д.

Далее, используя формулу (1), по паре символов (b_{q_t}, c_{q_t}) находим символ a_{q_t}, $t = 1,\dots,u$. Процедура расшифрования завершена.

Наконец, дадим обобщение предыдущей процедуры шифрования. Пусть алфавит состоит из m символов, причем имеет место представление $m = m_1\dots m_r$ с попарно простыми множителями $m_1, m_2, \dots, m_r$, превосходящими единицу. Определим числа M_s и M'_s следующими условиями

$$m_1m_2\dots m_r = M_sm_s, \quad M_sM'_s \equiv 1 \pmod{m_s}, \quad s = 1,2,\dots,r.$$

Положим

$$a = M_1M'_1b_1 + M_2M'_2b_2 + \dots + M_rM'_rb_r. \tag{2}$$

И пусть $b_1, b_2, \dots, b_r$ независимо друг от друга пробегают полные системы по модулям $m_1, m_2, \dots, m_r$ соответственно. Тогда a пробегает полную систему вычетов по модулю $m_1m_2\dots m_r$ (см., например, [8, гл. IV, § 3]).

Пусть, например, $m = 30$, $m = m_1m_2m_3 = 2\cdot3\cdot5 = 2\cdot15 = 3\cdot10 = 5\cdot6$. Тогда $M_1M'_1 \equiv 15\cdot1 \equiv 1 \pmod 2$, $M_2M'_2 \equiv 10\cdot1 \equiv 1 \pmod 3$, $M_3M'_3 \equiv 6\cdot1 \equiv 1 \pmod 5$.

Поэтому имеем $a \equiv 15b_1 + 10b_2 + 6b_3 \pmod{30}$.

Пусть, теперь, $b_{1,s}, b_{2,s}, \dots, b_{m_s,s}$ — полная система вычетов по модулю m_s, например, $1, 2, \dots, m_s, 1 \le s \le r$. Составим r таблиц Виженера для каждого из алфавитов $b_{1,s}, b_{2,s}, \dots, b_{m_s,s}$, $1 \le s \le r$.

Для каждой из приведенных выше таблиц Виженера при некотором натуральном числе t_s с условиями $1 \le t_s \le m_s$, задаем ключ $k_s = (b_{k_1,s}, b_{k_2,s}, \dots, b_{k_{t_s},s})$, $1 \le s \le r$.

Пусть, далее, задан открытый текст $a_{h_1}a_{h_2}\dots a_{h_u}$. По формуле (2) преобразуем его в r текстов. Имеем

$$b_{h_1,s}b_{h_2,s}\dots b_{h_u,s}, s = 1,2,\dots,r.$$

Аналогично вышеприведенному с помощью таблицы Виженера с номером s и ключа k_s шифруем текст $b_{h_1,s}b_{h_2,s}\dots b_{h_u,s}$, $s = 1, 2, \dots, r$. Расшифрование проводится также аналогично вышеизложенному.

7. Арифметический вариант шифра Виженера

Рассмотрим один из возможных путей обобщения шифра Виженера [7, 12], использующий возможность аддитивного представления целых чисел. Пусть m — количество всех символов алфавита и для натуральных чисел m, m_1, m_2 справедливы равенства $m = m_1 m_2$, $(m_1, m_2) = 1$, $m_1 > 1, m_2 > 1$. Например, $m = 30$, $m_1 = 5$, $m_2 = 6$.

Далее, пусть α_1 пробегает полную систему вычетов по модулю m_2, а α_2 — полную систему вычетов по модулю m_1. Тогда сумма $m_1\alpha_1 + m_2\alpha_2$ пробегает полную систему вычетов по модулю m [14]. Другими словами, любое целое число a с условием $1 \le a \le m$ при некоторых фиксированных b_1 по модулю m_2 и b_2 по модулю m_1 единственным образом представляется в виде

$$a \equiv b_1 m_1 a_1 + b_2 m_2 a_2 \pmod{m}, \tag{3}$$

где $1 \le a_1 \le m_2$, $1 \le a_2 \le m_1$, находятся из сравнений $b_1 m_1 a_1 \equiv a \pmod{m_2}$ и $b_2 m_2 a_2 \equiv a \pmod{m_1}$.

Таким образом, каждому целому числу a, $1 \le a \le m$, отвечает единственная пара целых чисел (a_1, a_2), удовлетворяющая сравнению (3). Расположение пар (a_1, a_2) в указанном выше соответствии может служить частью секретного ключа. По формуле (3) этот ключ однозначно задается парой (b_1, b_2), где $1 \le b_1 \le m_2, 1 \le b_2 \le m_1$. Следовательно, число возможных ключей равно $m = m_1 m_2$.

Более того, каждому символу a алфавита можно поставить некоторым образом в соответствие любую пару (β_1, β_2) с условием $1 \le \beta_1 \le m_2, 1 \le \beta_2 \le m_1$. Тогда число всевозможных ключей будет равно $m_1!m_2!$.

Далее, составим таблицу Виженера по следующему правилу: в строку с номером k поместим элементы $((\beta_1 + ck) \pmod{m_2}, (\beta_2 + ck) \pmod{m_1})$, где различные пары $(\beta_1 \pmod{m_2}, \beta_2 \pmod{m_1})$ образуют первую строку, величина k изменяется от 0 до $m-1$ и c — любое целое число, взаимно простое с m. Для того, чтобы полученная таблица была таблицей Виженера необходимо и достаточно, чтобы строки с разными номерами были различными. Предположим, что в построенной таблице строки с номерами k и k' совпадают. Тогда, очевидно, имеем $c(k - k') \equiv 0 \pmod{m_2}$, $c(k - k') \equiv 0 \pmod{m_1}$. Отсюда получим, что $m \mid (k - k')$. Это означает, что $k = k'$. Тем самым доказано, что построенная таблица является таблицей Вижене-

ра. Отметим, что число c также может служить частью секретного ключа.

Шифрование и дешифрование по построенной таблице осуществляется стандартным образом.

Обратим внимание еще на один момент составления таблицы Виженера. Пусть количество символов алфавита равно m, число m представляется в виде $m = m_1 \dots m_r$, $r \geq 2$, и m_k, m_l попарно взаимно просты при $k, l = 1, \dots, r$. Далее, каждому символу a, являющемуся вычетом по модулю m, взаимно однозначным образом поставим в соответствие набор $(a_1, \dots, a_r)$, где a_k, $k = 1, \dots, r$, принимает значения из полной системы вычетов по модулю m_k. Например, это соответствие можно установить следующим образом. Положим $M_k = mm_k^{-1}$. Тогда любой вычет a по модулю m однозначным образом представляется в виде $a \equiv M_1 a_1 + \dots + M_r a_r \pmod{m}$, где a_k, $k = 1, \dots, r$, принимает значения из полной системы вычетов по модулю m_k. Различным наборам $(a_1, \dots, a_r)$, где $0 \leq a_k < m_k$, $k = 1, \dots, r$, отвечают различные вычеты a по модулю m. Таким образом, при указанных соответствиях существует $m_1! \dots m_r!$ секретных ключей.

По аналогии с предыдущим, составим таблицу Виженера по следующему правилу: в строку с номером k поместим элементы $((a_1 + ck) \pmod{m_1}, \dots, (a_r + ck) \pmod{m_r})$, где различные пары $(a_1 \pmod{m_1}, \dots, a_r \pmod{m_r})$ образуют первую строку, величина k изменяется от 0 до $m-1$ и c — любое целое число, взаимно простое с m. Строки с разными номерами в этой таблице будут различными, так что получена таблица Виженера.

Список литературы

1. Сингх С. Книга шифров: тайная история шифров и их расшифровки. — М.: АСТ: Астрель, 2007.

2. Алферов А. П., Зубов А. Ю., Кузьмин А. С., Черемушкин А. В. Основы криптографии: Учебное пособие. 2-е изд., испр. и доп. — М.: Гелиос АРВ, 2002.

3. Минеев М. П., Чубариков В. Н. Задача об искажении частоты появления знаков в шифре простой замены // Математические вопросы кибернетики. Вып. 16. — 2007. — С. 242–245.

4. Минеев М. П., Чубариков В. Н. Об одном методе искажения частоты появления знаков в шифре простой замены // Докл. РАН. — 2008. — Т. 420, № 6. — С. 736–738.

5. Минеев М. П., Чубариков В. Н. К вопросу об искажении частот появления знаков в шифре простой замены // Докл. РАН. — 2009. — Т. 426, № 1. — С. 6–8.

6. Аршинов М. Н., Садовский Л. Е. Коды и математика. — М.: Наука, 1983.
7. Бабаш А. В., Шанкин Г. П. Криптография. — М.: СОЛОН-Пресс, 2007.
8. Баричев С. Криптография без секретов [Электронный ресурс]. — http://www.artelecom.ru/library/books/swos/index/html.
9. Жельников В. Криптография от папируса до компьютера. — М.: ABF, 1996.
10. Молдовян А. А., Молдовян Н. А., Советов Б. Я. Криптография. — СПб.: Лань, 2001.
11. Саломаа А. Криптография с открытым ключом. — М.: Мир, 1996.
12. Нечаев В. И. Элементы криптографии (Основы теории защиты информации): Учеб. пос. для ун-тов и пед. вузов — М.:Высш.шк., 1999.
13. Коблиц Н. Курс теории чисел и криптографии. — М.: Научное изд-во ТВП, 2001.
14. Виноградов И. М. Основы теории чисел. — М.: Наука, 1983.
15. Гашков С. Б., Чубариков В. Н. Арифметика. Алгоритмы. Сложность вычислений. — М.: Наука, 1996.
16. Чубариков В. Н. Элементы арифметики. — М.: Изд-во Механико-математического ф-та МГУ, 2007.

О НЕКОТОРЫХ ЗАДАЧАХ В ОБЛАСТИ МНОГОЗНАЧНЫХ ЛОГИК

А. Б. Угольников (Москва)

Основным объектом исследований является множество P_k всех функций[1] k-значной логики, $k \geq 2$. Обозначим через $\mathcal{B} = \mathcal{B}(P_k)$ множество всех подмножеств множества P_k. Представим на примере этого множества некоторые задачи теории функциональных систем.

Рассмотрим отображение $\varphi : \mathcal{B} \to \mathcal{B}$, такое, что для любой системы $\mathfrak{A} \subseteq P_k$ множество $\varphi(\mathfrak{A})$ состоит из всех функций k-значной логики, реализуемых нетривиальными формулами над $\mathfrak{A}$; при этом равенство функций понимается в следующем смысле: функции равны, тогда и только тогда, когда они зависят от одного и того же

[1] *Функцией k-значной логики* называется функция $f(x_1, x_2, \ldots, x_n)$, $n \geq 1$, определённая на множестве E_k^n и принимающая значения из множества E_k, где $E_k = \{0, 1, \ldots, k-1\}$, $k \geq 2$.

множества переменных и на любом наборе значений этих переменных принимают одинаковые значения. Легко видеть, что это отображение удовлетворяет следующим свойствам (называемым также *аксиомами*):

(1) $\mathfrak{A} \subseteq \varphi(\mathfrak{A})$,

(2) если $\mathfrak{A} \subseteq \mathfrak{B}$, то $\varphi(\mathfrak{A}) \subseteq \varphi(\mathfrak{B})$,

(3) $\varphi(\varphi(\mathfrak{A})) = \varphi(\mathfrak{A})$

для всех $\mathfrak{A}, \mathfrak{B} \in \mathcal{B}$. Поэтому отображение φ является оператором замыкания [1]. Этот оператор называется также оператором (или *операцией*) *суперпозиции*.

В результате получаем функциональную систему $\mathcal{P}_k = (P_k; \varphi)$, состоящую из множества P_k всех функций k-значной логики и оператора суперпозиции φ, отображающего множество $\mathcal{B}(P_k)$ в себя.

Положим[2] $\mathcal{B}_\varphi = \{\varphi(\mathfrak{A}) \,|\, \mathfrak{A} \in \mathcal{B}\}$. Пусть $F \in \mathcal{B}_\varphi$, $\mathfrak{A} \subseteq P_k$. Будем говорить, что система $\mathfrak{A}$ *порождает* множество F ($\mathfrak{A}$ — *порождающая система* F или $\mathfrak{A}$ является *полной* в F), если $\varphi(\mathfrak{A}) = F$. Будем называть систему $\mathfrak{A}$ *базисом* множества F, если $\mathfrak{A}$ порождает F и для любой системы $\mathfrak{A}' \subset \mathfrak{A}$ выполняется соотношение $\varphi(\mathfrak{A}') \neq F$.

Множество $F \subseteq P_k$ называется *замкнутым относительно оператора* φ, если $\varphi(F) = F$. Замкнутые множества называются также *замкнутыми классами* (относительно φ).

Получаем следующие основные задачи.

1. Задача *о выразимости*: по заданной системе $\mathfrak{A} \subseteq P_k$ и произвольной функции f из P_k установить, принадлежит f множеству $\varphi(\mathfrak{A})$ или нет.
2. Задача *о полноте*: для заданного множества $F \in \mathcal{B}_\varphi$ и произвольной системы $\mathfrak{A} \subseteq P_k$ определить, порождает $\mathfrak{A}$ множество F или нет.

Можно выделить также следующие два уточнения задачи о полноте:

2*a*) задача *о конечной порождённости*: для заданного множества $F \in \mathcal{B}_\varphi$ определить, имеет F конечную порождающую систему или нет;

2*b*) задача *о базируемости*: для заданного множества $F \in \mathcal{B}_\varphi$ определить, имеет F базис или нет.

Кроме того, возникает серия задач под общим названием:

3. *Описание свойств* семейства $\mathcal{B}_\varphi$.

[2] То есть $\mathcal{B}_\varphi$ состоит из всех подмножеств F множества P_k, таких, что для некоторой системы $\mathfrak{A} \subseteq P_k$ выполнено равенство $\varphi(\mathfrak{A}) = F$.

К их числу можно отнести, например, следующие задачи: определить мощность семейства $\mathcal{B}_\varphi$, построить фрагменты диаграммы включений и т. д.

Следует отметить, что все эти задачи (как и все определённые выше понятия) можно сформулировать также и для других функциональных систем $(P;\psi)$, где P — некоторое множество, а ψ — некоторое отображение множества $\mathcal{B}(P)$ всех подмножеств множества P в себя.

Для функциональной системы $\mathcal{P}_2 = (P_2;\varphi)$ ответы на эти вопросы были получены в 1920 году американским математиком Э. Л. Постом[3] [2–4]. Он описал все замкнутые относительно операции суперпозиции классы булевых функций и показал, что каждый такой класс имеет конечный базис.

В книге С. В. Яблонского, Г. П. Гаврилова и В. Б. Кудрявцева [5] было дано более компактное и простое изложение этих результатов. При этом в отличие от работ Поста в книге [5] предполагается, что всякое множество вместе с каждой функцией содержит также и все функции, отличающиеся от неё фиктивными переменными. То есть фактически рассматривается функциональная система $\mathcal{P}_2^+ = (P_2;\varphi^+)$, в которой замыкание систем функций осуществляется относительно двух операций: суперпозиции и введения фиктивной переменной[4]. Такой подход позволил получить более простую структуру замкнутых классов, чем структура, описанная у Поста. В ней отсутствуют классы (их семнадцать), которые не являются замкнутыми относительно операции введения несущественной переменной.

Описание классов Поста содержится также в [6–13]. Алгебраический подход к понятиям суперпозиции и замкнутого класса предложен А. И. Мальцевым [14, 15].

Проведение аналогичных исследований при $k \geq 3$ наталкивается на значительные трудности, поскольку известны результаты, показывающие принципиальные отличия многозначных логик от двузначной. К их числу относятся примеры Ю. И. Янова о существовании в P_k при $k \geq 3$ замкнутых классов, не имеющих базиса, и А. А. Мучника о существовании замкнутых классов со счётным базисом (см. [16], 1959 г.). Из этих результатов, в частности, следует континуальность семейства $\mathcal{B}_{\varphi^+}$ всех замкнутых классов в функциональной системе $\mathcal{P}_k^+ = (P_k;\varphi^+)$ при всех $k \geq 3$ (см. также [17, 18]).

[3] Следует отметить, что подробное изложение этих результатов содержится в работе [4]; в [2, 3] они лишь анонсированы.

[4] Иными словами множество $\varphi^+(\mathfrak{A})$ состоит из всех булевых функций, реализуемых нетривиальными формулами над $\mathfrak{A}$, а также всех функций, отличающихся от них несущественными переменными, $\mathfrak{A} \subseteq P_2$.

В связи с этим можно выделить следующие два важных направления исследований.

I. Изучение свойств конкретных семейств замкнутых классов.

II. Изучение функциональных систем, в которых операторы являются некоторым "усилением" оператора суперпозиции.

Рассмотрим сначала задачи, относящиеся к направлению I.

1. Среди семейств замкнутых классов в функциональной системе $\mathcal{P}_k^+$ одно из центральных мест занимает семейство предполных классов[5]. Перечислим некоторые результаты, полученные в этом направлении.

С. В. Яблонский [19, 20] нашёл все предполные классы в P_3. Конечность числа предполных классов в P_k при всех $k \geq 3$ установил А. В. Кузнецов [21, 22]. Некоторые семейства предполных классов найдены в работах [23–30]. Описание всех предполных классов в P_k при всех $k \geq 3$ получено И. Розенбергом в 1965 году [31, 32].

Описание этих классов содержится также в [13, 33–36]. В соответствии с ним в P_k имеются следующие семейства предполных классов[6]:

1) классы самодвойственных функций — классы типа $\mathbb{P}$;
2) классы линейных функций — классы типа $\mathbb{L}$;
3) классы функций, сохраняющих разбиение множества E_k, — классы типа $\mathbb{E}$;
4) классы функций, сохраняющих центральные отношения, — классы типа $\mathbb{C}$;
5) классы монотонных функций — классы типа $\mathbb{O}$;
6) классы функций, сохраняющих сильно гомоморфные прообразы h-адических элементарных отношений, — классы типа $\mathbb{B}$.

Рассмотрим задачу о конечной порождённости для предполных классов функций.

В работе Д. Лау [37] исследованы порядки[7] предполных классов в P_k и, в частности, указаны конечные порождающие системы при $k \geq 3$ для всех предполных классов типа $\mathbb{L}$, $\mathbb{P}$, $\mathbb{E}$, $\mathbb{C}$ и $\mathbb{B}$, а также при $k \leq 7$ для всех предполных классов типа $\mathbb{O}$ (см. также [13, 20, 23–25, 32, 36, 38–43]). В 1986 году Г. Тардош [44] привёл пример частично

[5] Замкнутый класс F называется *предполным* (в P_k), если $F \neq P_k$ и для любой функции $f \notin F$ выполняется равенство $\varphi^+(F \cup \{f\}) = P_k$.

[6] Здесь используются обозначения из книги [36].

[7] Порядком конечно-порождённого класса F называется наименьшее натуральное r, при котором множество $F(r)$ всех функций $f(x_1, x_2, \ldots, x_r)$ из F порождает F (т. е. выполняется равенство $\varphi^+(F(r)) = F$).

упорядоченного множества $R = \{0, \alpha, \alpha', \beta, \beta', \gamma, \gamma', 1\}$ из 8 элементов (см. рис. 1) и показал, что класс M_R (предполный класс в P_8) всех функций, монотонных относительно множества R, не имеет конечного базиса.

Таким образом, возникает задача о получении необходимых и достаточных условий конечной порожденности для предполных классов типа $\mathbb{O}$.

К настоящему времени получен ряд достаточных условий конечной порождённости таких классов. В частности, из теоремы К. Бейкера и А. Пиксли [45] следует, что всякий замкнутый класс, содержащий мажоритарную функцию, является конечно-порождённым (см. также [13]). Известны также некоторые достаточные условия для частично упорядоченных множеств, при выполнении которых соответствующие классы монотонных функций являются конечно-порождёнными (см., например, [46, 47]).

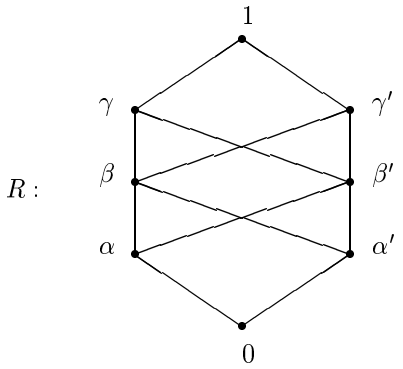


Рис. 1

Существенное продвижение в решении этой задачи получено в работах О. С. Дудаковой [48–50], в которых приводится критерий конечной порождённости для всех предполных классов функций, монотонных относительно частично упорядоченных множеств ширины[8] 2.

Обозначим через $\mathcal{R}$ семейство всех частично упорядоченных множеств ширины 2 с наибольшим и наименьшим элементами, а через M_R — класс[9] всех функций, монотонных относительно множества R, $R \in \mathcal{R}$.

[8] Шириной частично упорядоченного множества называется максимальное число его попарно несравнимых элементов.

[9] Известно [23], что все такие классы являются предполными.

Пусть a и b — несравнимые элементы множества Q, $Q \in \mathcal{R}$. Если эти элементы имеют точную верхнюю грань, то обозначим её через $\sup(a,b)$. Пусть (несравнимые) элементы a и b не имеют точной верхней грани, пусть c и d — две минимальные верхние грани элементов a и b и пусть существует точная верхняя грань h элементов c и d. Тогда h называется *точной верхней гранью второго порядка* элементов a и b и обозначается через $\sup^2(a,b)$ (т. е. $\sup^2(a,b) = \sup(c,d) = h$).

В [50] доказано следующее утверждение: для любого множества $Q \in \mathcal{R}$ класс M_Q всех функций, монотонных относительно Q, имеет конечный базис тогда и только тогда, когда любые два несравнимых элемента $a, b \in Q$ имеют или $\sup(a,b)$ или $\sup^2(a,b)$.

В частности, из этого критерия извлекается простой полиномиальный алгоритм проверки существования конечного базиса у класса M_Q в терминах свойств элементов множества Q. Из этого результата также следует, что достаточные условия конечной порождённости для предполных классов монотонных функций, приведённые в работах [46, 47], не являются необходимыми.

Некоторые условия конечной порождённости для предполных классов функций многозначной логики, монотонных относительно частично упорядоченных множеств из ряда других семейств, получены в [51, 52].

Следует отметить, что метод, приведённый в работе Тардоша, не позволяет дать ответ на вопрос[10] о базируемости класса M_R. Это говорит о недостатке имеющихся средств для решения подобных задач.

2. Рассмотрим задачи о конечной порождённости и о базируемости в более общей постановке.

Пусть $\mathfrak{A} \subseteq \mathfrak{M} \subseteq P_k$, $G = [\mathfrak{A}]$. Возникает вопрос, какой из следующих трёх случаев имеет место: G имеет конечный базис, G имеет счётный базис или G не имеет базиса. Иными словами, из некоторых соображений выбирается множество $\mathfrak{M} \subseteq P_k$ и для замкнутых классов, порождённых системами функций из $\mathfrak{M}$, рассматриваются задачи о базируемости и о конечной порождённости. Естественно, что подобные вопросы могут быть поставлены для различных подмножеств множества P_k. В частности, при $\mathfrak{M} = P_k$ получаем упомянутые выше задачи $2a$ и $2b$.

Рассмотрим задачу в данной постановке для более "простых" систем $\mathfrak{M}$ ($\mathfrak{M} \neq P_k$). В качестве отправной точки рассмотрим классы Янова — Мучника. Напомним определение этих классов.

[10] Этот вопрос в настоящее время является открытым.

Пусть $k \geq 3$, $n \geq 2$. Положим

$$H_n = \{(\alpha_1, \ldots, \alpha_n) \in E_k^n \mid \alpha_1 = \ldots = \alpha_{i-1} = \alpha_{i+1} = \ldots = \alpha_n = 2, \alpha_i = 1,\ i = 1, 2, \ldots, n\}.$$

Определим последовательности функций $f_1, f_2, \ldots$ и $g_2, g_3, \ldots$ из P_k следующим образом. Положим

$$f_m(x_1, x_2, \ldots, x_m) = \begin{cases} 1 \text{ при } x_1 = x_2 = \ldots = x_m = 2, \\ 0 \text{ в остальных случаях,} \end{cases}$$

$$g_n(x_1, x_2, \ldots, x_n) = \begin{cases} 1 \text{ при } (x_1, x_2, \ldots, x_n) \in H_n, \\ 0 \text{ в остальных случаях,} \end{cases}$$

где $m \geq 1$, $n \geq 2$.

Классы F_k и G_k (классы Янова и Мучника соответственно) при всех $k \geq 3$ определяются следующим образом: $F_k = \varphi^+(\mathfrak{F}_k)$, $G_k = \varphi^+(\mathfrak{G}_k)$, где

$$\mathfrak{F}_k = \bigcup_{m \geq 1} \{f_m\}, \quad \mathfrak{G}_k = \bigcup_{n \geq 2} \{g_n\}.$$

Легко видеть, что для замкнутых классов, порождающие системы которых являются подмножествами множеств $\mathfrak{F}_k$ или $\mathfrak{G}_k$, поставленные выше вопросы имеют тривиальное решение. В самом деле, если $\mathfrak{A} \subseteq \mathfrak{F}_k$, $A = \varphi^+(\mathfrak{A})$, то A имеет базис тогда и только тогда, когда множество $\mathfrak{A}$ конечно. Аналогично, если $\mathfrak{B} \subseteq \mathfrak{G}_k$, $B = \varphi^+(\mathfrak{B})$, то B имеет базис; при этом B имеет счётный базис тогда и только тогда, когда множество $\mathfrak{B}$ бесконечно.

Пусть $k \geq 3$. Обозначим через $P_{k,2}$ множество всех функций k-значной логики, принимающих значения только из множества $\{0,1\}$ (см. [13, 53–58]), через R_k — множество всех функций $f(x_1, \ldots, x_n)$ из $P_{k,2}$ ($n \geq 1$), равных нулю на единичном наборе, а также на всех наборах из E_k^n, имеющих по крайней мере одну нулевую компоненту, через S_k — множество всех симметрических функций из R_k, через S_k^m — множество всех m-слойных[11] симметрических функций из R_k, $m \geq 1$, а через NS_k^1 — множество всех функций из S_k^1, равных нулю на всех наборах вида $(a, a, \ldots, a)$, $a \in E_k$. Очевидно, что

$$NS_k^1 \subseteq S_k^1 \subseteq S_k \subseteq R_k \subseteq P_{k,2}.$$

[11] Функция из множества R_k называется *m-слойной симметрической* функцией, если существуют m слоёв, $m \geq 1$, таких, что она равна единице на всех наборах из этих слоёв и равна нулю на всех остальных наборах; *слоем* называется множество наборов из E_k^n, получающихся друг из друга перестановкой компонент наборов, $n \geq 1$.

Итак, классы F_k и G_k (Янова—Мучника) — первые примеры классов в P_k, не имеющих конечного базиса. Эти классы являются "простейшими" с точки зрения ответов на поставленные вопросы. И, кроме того, их порождающие системы $\mathfrak{F}_k$ и $\mathfrak{G}_k$ соответственно обладают рядом интересных свойств:

1) $\mathfrak{F}_k, \mathfrak{G}_k \subseteq P_{k,2}$, причём $\mathfrak{F}_k, \mathfrak{G}_k \subseteq R_k$;
2) $\mathfrak{F}_k, \mathfrak{G}_k \subseteq S_k$, причём $\mathfrak{F}_k \subseteq S_k^1$, $\mathfrak{G}_k \subseteq NS_k^1 \subseteq S_k^1$;
3) для любых $\mathfrak{A}, \mathfrak{B} \subseteq \mathfrak{F}_k$ и любых $\mathfrak{C}, \mathfrak{D} \subseteq \mathfrak{G}_k$ выполняются равенства
$$\varphi^+(\mathfrak{A} \cup \mathfrak{B}) = \varphi^+(\mathfrak{A}) \cup \varphi^+(\mathfrak{B}), \quad \varphi^+(\mathfrak{C} \cup \mathfrak{D}) = \varphi^+(\mathfrak{C}) \cup \varphi^+(\mathfrak{D}).$$

Исследования в данном направлении проведены в работах А. В. Михайлович [59–61]. В этих работах изучаются континуальные семейства классов, порождаемых системами функций многозначной логики, обладающих свойствами, которые аналогичны свойствам функций из систем $\mathfrak{F}_k$ и $\mathfrak{G}_k$. Для рассматриваемых замкнутых классов в терминах отношений частичного порядка, которые определяются на множествах функций, получены критерии базируемости и конечной порожденности, кроме того, описан ряд других важных свойств этих классов.

Приведём некоторые из этих результатов.

Функции f и g из P_k называются *конгруэнтными*, если одну из них можно получить из другой переименованием переменных без отождествления (обозначение $f \cong g$). Пусть $A \subseteq P_k$, $f \in A$. Положим $\mathcal{F}_A(f) = \{g \in A | g \cong f\}$,

$$\mathcal{F}_A = \bigcup_{f \in A} \{\mathcal{F}_A(f)\}.$$

Очевидно, что $\mathcal{F}_A$ является разбиением множества A на классы, состоящие из конгруэнтных функций. Пусть на множестве $\mathcal{F}_A$ задано некоторое отношение частичного порядка $\preceq_A$, $f, g \in A$ и пусть $\mathcal{F}_A(f) \preceq_A \mathcal{F}_A(g)$. Будем также писать $f \preceq_A g$, сравнивая функции f и g как представителей классов $\mathcal{F}_A(f)$ и $\mathcal{F}_A(g)$ соответственно, и $f \prec_A g$, если $f \preceq_A g$ и $f \not\cong g$.

Пусть $\alpha \in \mathbb{Q}^+$, $f \in S_3^1$. Будем говорить, что f является функцией типа σ, если отношение числа единиц к числу двоек в слое, на наборах которого функция f принимает значение 1, равно σ.

Определим отношение $\preceq_{S_3^1}$ на множестве $\mathcal{F}_{S_3^1}$ следующим образом. Пусть $f(x_1, \ldots, x_n)$, $g(y_1, \ldots, y_p) \in S_3^1$. Будем использовать обозначение $\mathcal{F}_{S_3^1}(f) \preceq_{S_3^1} \mathcal{F}_{S_3^1}(g)$, если f и g — функции одного типа и p

кратно n. Очевидно, что отношение $\preceq_{S_3^1}$ транзитивно, рефлексивно и антисимметрично. Поэтому оно является отношением частичного порядка [62] на множестве $\mathcal{F}_{S_3^1}$.

В работах [59, 61] показано, что для произвольного множества G, состоящего из попарно неконгруэнтных функций множества NS_3^1, класс $F = \varphi^+(G)$ имеет базис тогда и только тогда, когда каждая функция из G содержится в некоторой ограниченной максимальной цепи относительно отношения $\preceq_{S_3^1}$; при этом F имеет конечный базис тогда и только тогда, когда множество G конечно.

Аналогичные критерии получены также для множества MS всех симметрических функций из R_3, монотонных относительно порядка $0 < 1 < 2$.

Пусть $f \in MS$. Обозначим через e_f число единиц в слое с наибольшим числом единиц, на котором функция f принимает значение 1. Пусть $G \subseteq MS$, $k \in \mathbb{Z}^+$. Множество G называется *k-ограниченным*, если для любой функции $f \in G$ выполняется неравенство $e_f \leq k$ и найдётся функция $g \in G$, такая, что $e_g = k$. Далее, пусть G — k-ограниченное множество. Положим $\mathcal{K}(G) = \{g \in G | e_g = k\}$.

Определим отношение $\preceq_{MS}$ на множестве $\mathcal{F}_{MS}$. Пусть $f, g \in MS$. Будем использовать обозначение $\mathcal{F}_{MS}(f) \preceq_{MS} \mathcal{F}_{MS}(g)$, если $f \in \varphi^+(\{g\})$.

В [60, 61] показано, что отношение $\preceq_{MS}$ является отношением частичного порядка на множестве $\mathcal{F}_{MS}$, и доказано следующее утверждение: для произвольного множества G, состоящего из попарно неконгруэнтных функций множества MS, класс $F = \varphi^+(G)$ имеет базис тогда и только тогда, когда каждая функция из G содержится в некоторой ограниченной цепи множества G относительно отношения $\preceq_{MS}$; при этом F имеет конечный базис тогда и только тогда, когда для некоторого $k \in \mathbb{Z}^+$ множество G является k-ограниченным и множество $\mathcal{K}(G)$ конечно.

Аналогичные критерии получены также для $NS_3^m = S_3^m \setminus MS$, NS_k^1, $m \geq 1$, $k \geq 3$, и некоторых других множеств симметрических функций.

Следует отметить, что поскольку $\mathfrak{F}_3 \subseteq MS$, $\mathfrak{G}_3 \subseteq NS_3^1$, то

$$F_3 \in \mathcal{B}_{\varphi^+}(MS), \quad G_3 \in \mathcal{B}_{\varphi^+}(NS_3^1),$$

где $\mathcal{B}_{\varphi^+}(MS)$ и $\mathcal{B}_{\varphi^+}(NS_3^1)$ — семейства замкнутых классов, порождающие системы которых являются подмножествами множеств

MS и NS_3^1 соответственно. Таким образом, на основе классов Янова и Мучника (при $k = 3$) построены другие ("расширенные") множества функций трёхзначной логики — множества MS и NS_3^1 соответственно; при этом для замкнутых классов, порождённых системами функций, принадлежащих этим множествам, получены критерии базируемости и конечной порождённости.

В связи с этими результатами возникает, в частности, вопрос об описании всех множеств $\mathfrak{M} \subseteq P_k$, таких, что для любых $\mathfrak{A}, \mathfrak{B} \subseteq \mathfrak{M}$ выполняется свойство

(4) $\varphi^+(\mathfrak{A} \cup \mathfrak{B}) = \varphi^+(\mathfrak{A}) \cup \varphi^+(\mathfrak{B})$

(в дополнение к аксиомам (1)–(3), указанным выше).

Перейдём теперь к задачам, относящимся к направлению II.

3. В задачах этого направления рассматриваются функциональные системы с различными усилениями оператора суперпозиции. Такой подход[12] позволяет получить более обозримую структуру классов, замкнутых относительно рассматриваемого оператора замыкания. Среди исследований, проведённых в этом направлении, можно отметить, например, работы [63–68], в которых рассматривается операция S-замыкания, и работы [69–72], в которых изучаются функциональные системы с операциями замыкания программного типа.

Следует отметить, что все перечисленные примеры операторов замыкания (за исключением некоторых операций программного типа) приводят к конечному множеству замкнутых классов в P_k при всех $k \geq 3$, что говорит об излишней "выразительной силе" рассматриваемых операций. Поэтому представляется важным построение таких функциональных систем (P_k, ψ), в которых оператор ψ:

1) является усилением оператора суперпозиции,
2) "возникает" при решении других задач,
3) позволяет получить новые "эффекты" при изучении свойств семейства $\mathcal{B}_\psi$.

К числу таких усилений операции суперпозиции можно отнести добавление к ней операции перестановки, которая использует геометрический способ представления функций и даёт простой способ вычисления результата. Операция перестановки определяется на основе разбиения множества E_k^n на непересекающиеся подмножества $B_1, B_2, \ldots, B_m$, $n, m \geq 1$. При этом на каждом B_i, $1 \leq i \leq m$, задаётся взаимно однозначное отображение множества B_i в себя, что

[12] Подобный путь, в частности, намечен в книге [5], в которой операция суперпозиции дополнена операцией введения фиктивной переменной.

позволяет переставлять значения функций на наборах этого подмножества.

Операции такого вида возникали, например, в работах [73, 74] при перечислении монотонных булевых функций и в работах автора [75–77] при реализации монотонных функций из классов Поста схемами из функциональных элементов в полных конечных базисах.

Подобные усиления операции суперпозиции подробно исследованы в работах О. С. Тарасовой [78–80]. В этих работах рассматривается несколько видов разбиений множества E_k^n на подмножества, $n \geq 1$, и два типа отображений (полученных на основе перестановок компонент наборов и отображения произвольного вида). Кроме того, рассматривается ограничение на область применения рассматриваемых операций, связанное с наличием у функций фиктивных переменных. В [78–80] для каждого случая описан ряд важных свойств соответствующих семейств замкнутых классов. В частности, приведён пример функциональной системы $(P_k; \pi)$, в которой семейство $\mathcal{B}_\pi$ замкнутых (относительно π) классов в P_k является счётным при всех $k \geq 3$.

Отметим один из наиболее интересных результатов. Рассматриваются разбиения множества E_n^k, $n \geq 1$, на слои относительно угловых наборов и ослабленная операция перестановки (то есть операцию можно применять только к функциям, существенно зависящим от всех своих переменных). В работах [79, 80] показано, что при $k = 3$ для любого множества угловых наборов, удовлетворяющего некоторым условиям, соответствующее семейство замкнутых классов является счётным, а при всех $k \geq 5$ континуальным (вопрос о мощности этого семейства при $k = 4$ в настоящее время остаётся открытым).

Таким образом, приведён пример оператора замыкания, который (являясь усилением оператора суперпозиции) демонстрирует существенные отличия P_3 от P_k при всех $k \geq 5$ (то есть "отделяет" P_3 от P_5).

Следует также отметить, что в функциональных системах такого типа одновременное выполнение следующих двух условий: наличие операции введения фиктивных переменных и отсутствие ограничений на область применения операции перестановки — приводит к конечному числу замкнутых классов при всех $k \geq 2$.

Работа выполнена при финансовой поддержке РФФИ (проект 08–01–00863) и программы поддержки ведущих научных школ РФ (проект НШ–4437.2010.1).

Список литературы

1. Кон П. Универсальная алгебра. — М.: Мир, 1968.

2. Post E. L. Determination of all closed systems of truth tables // Abstract. Bull. Amer. Math. Soc. — 1920. — V. 26, № 10. — P. 437. [Reprinted in: Solvability, provability, definability: the collected works of Emil L. Post / Martin Davis editor. Boston, Basel, Berlin: Birkhauser, 1994. — P. 545.]

3. Post E. L. Introduction to a general theory of elementary propositions (Doctoral dissertation, Columbia University, 1920) // Amer. J. Math. — 1921. — V. 43, № 3, July. — P. 163–185. [Reprinted in: ibid. — P. 21–43.].

4. Post E. L. Two-valued iterative systems of mathematical logic // Ann. Math. Stud. Princeton; London: Princeton Univ. Press, 1941. — № 5. [Reprinted in: ibid. — P. 249–374.]

5. Яблонский С. В., Гаврилов Г. П., Кудрявцев В. Б. Функции алгебры логики и классы Поста. — М.: Наука, 1966.

6. Угольников А. Б. О замкнутых классах Поста // Изв. вузов. Математика. — 1988. — № 7 (314). — С. 79–88.

7. Марченков С. С., Угольников А. Б. Замкнутые классы булевых функций. — М.: ИПМ АН СССР, 1990.

8. Марченков С. С. Замкнутые классы булевых функций. — М.: Физматлит, 2000.

9. Угольников А. Б. Классы Поста. — М.: Изд-во ЦПИ при мех.-матем. ф-те МГУ им. М. В. Ломоносова, 2008.

10. Kuntzman J. Algèbre de Boole. — Paris: Dunod, 1965.

11. Rescke M., Denecke K. Ein neuer Beweis für die Ergebniss von E. L. Post über abgeschlossene Klassen Boolescher Funktionnen // J. Process. Cybern. EIK. — 1989. — Bd. 25, 7. — S. 361–380.

12. Lau D. On closed subsets of Boolean functions (A new proof for Post's theorem) // J. Process. Cybern. EIK. — 1991. — V. 27, 3. — P. 167–178.

13. Lau D. Function algebras on finite sets. — Berlin; Heiderbelg: Springer-Verlag, 2006.

14. Мальцев А. И. Итеративные алгебры и многообразия Поста // Алгебра и логика. — Новосибирск, 1966. — Т. 5, № 2. — С. 5–24.

15. Мальцев А. И. Итеративные алгебры Поста. — Новосибирск: Изд-во НГУ, 1976. Вып. 16.

16. Янов Ю. И., Мучник А. А. О существовании k-значных замкнутых классов, не имеющих конечного базиса // ДАН СССР. — 1959. — Т. 127, № 1. — С. 44–46.

17. Яблонский С. В. Введение в дискретную математику. — М.: Высшая школа, 2008.

18. Яблонский С. В. Введение в теорию функций k-значной логики // Дискретная математика и математические вопросы кибернетики. Т. I. — М.: Наука, 1974. — С. 9–66.

19. Яблонский С. В. О функциональной полноте в трёхзначном исчислении // ДАН СССР. — 1954. — Т. 95, № 6. — С. 1152–1156.

20. Яблонский С. В. Функциональные построения в k-значной логике // Труды матем. ин-та АН СССР им. Стеклова. — 1958. — Т. 51. — С. 5–142.

21. Кузнецов А. В. О проблемах тождества и функциональной полноты для алгебраических систем // Труды 3-го Всесоюзного матем. съезда. Т. 2. — М.: Изд-во АН СССР, 1956. — С. 145–146.

22. Кузнецов А. В. Алгебра логики и её обобщения // Математика в СССР за 40 лет (1917–1957). Т. 1. — М.: Физматгиз, 1959. — С. 102–115.

23. Мартынюк В. В. Исследование некоторых классов в многозначных логиках // Проблемы кибернетики. Вып. 3. — М.: Наука, 1960. — С. 49–60.

24. Байрамов Р. А. Об одной серии предполных классов в k-значной логике // Кибернетика. — Т. 1. — 1967. — С. 7–9.

25. Захарова Е. Ю. Критерий полноты систем функций из P_k // Проблемы кибернетики. Вып. 18. — М.: Наука, 1967. — С. 5–10.

26. Pan Jun-Cze. A solving method for finding all precomplete classes in many-valued logics // Acta Sci. Natur. Univ. Jilinensis. — 1962. — V. 2 (Chinese).

27. Lo Czukai. The precompleteness of a set and rings of linear functions // Acta Sci. Natur. Univ. Jilinensis. — 1963. — V. 2. — P. 1–14 (Chinese).

28. Lo Czukai. On the precompleteness of the classes of functions preserving a partition // Acta Sci. Natur. Univ. Jilinensis. — 1963. — V. 2. — P. 105–116 (Chinese).

29. Lo Czukai, Lju Sjui-Hua. Precomplete classes defined by binary relations in many-valued logics // Acta Sci. Natur. Univ. Jilinensis. — 1963. — V. 4. — P. 27–33 (Chinese).

30. Lo Czukai. Precomplete classes defined by normal k-ary relations in k-valued logics // Acta Sci. Natur. Univ. Jilinensis. — 1964. — V. 3. — P. 39–50 (Chinese).

31. Rosenberg I. G. La structure des functions de plusieurs variables sur un ensemble finil // Comptes Rendus, de l'Academ. Paris, Ser. A. B. — 260. — 1965. — P. 3817–3819.

32. Rosenberg I. G. Über die funktionale Vollständigkeit in den mehrvertigen Logiken. // Rozpravy Československě Academie věd. Rada matematickych a přirodnich věd. — Praha, 1970. — Ročnik 80, Sešit 4. — S. 3–93.

33. Кудрявцев В. Б. Функциональные системы. — М.: Изд-во МГУ, 1982.

34. Буевич В. А. Вариант доказательства критерия полноты для функций k-значной логики // Дискретная математика. — Т. 8, вып. 4. — 1996. — С. 11–36.

35. Марченков С. С. Предполнота замкнутых классов в P_k: предикатный подход // Математические вопросы кибернетики. Вып. 6. — М.: Наука. Физматлит, 1996. — С. 117–132.

36. Яблонский С. В., Гаврилов Г. П., Набебин А. А. Предполные классы в многозначных логиках. — М.: Изд-во МЭИ, 1997.

37. Lau D. Bestimmung der Ordnung maximaler Klassen von Funktionen der k-wertigen Logik // Z. math Log. und Grundl. Math. — 1978. — Bd. 24. — S. 79–96.

38. Гниденко В. М. Нахождение порядков предполных классов в трёхзначной логике // Проблемы кибернетики. Вып. 8. — М.: Физматгиз, 1962. — С. 341–346.

39. Кудрявцев В. Б. О покрытиях предполных классов k-значной логики // Дискретный анализ. — Вып. 17. — 1970. — С. 32–44.

40. Сафин Р. Ф. О равномерности систем монотонных функций // Вестн. Моск. ун-та. Серия 1. Матем. Механ. — 2003. — № 2. — С. 15–20.

41. Сафин Р. Ф. О соотношении между глубиной и сложностью формул в предполных классов k-значной логики // Математические вопросы кибернетики. Вып. 13. — 2004. — С. 223–278.

42. Schofield P. Independent conditions for completeness of finite algebras with a single generator // J. London Math. Soc. — 1969. — V. 44. — P. 413–423.

43. Pöschel R., Kaluznin L. A. A. Funktionen- und Relationenalgebren. — Berlin: VEB Deutscher Verlag der Wissenschaften, 1979.

44. Tardos G. A not finitely generated maximal clone of monotone operations // Order. — 1986. — 3. — P. 211–218.

45. Baker K. A., Pixley A. F. Polynomial interpolation and the chinese remainder theorem for algebraic systems // Math. Z. — 1975. — 143. — P. 165–174.

46. Demetrovics J., Hannák L., Rónyai L. Near unanimity functions and partial orderings // Proc. 14 ISMVL, Manitoba. — 1984. — P. 52–56.

47. Demetrovics J., Hannák L., Rónyai L. On algebraic properties of monotone clones // Order. — 1986. — 3. — P. 219–225.

48. Дудакова О. С. О свойствах предполных классов монотонных функций k-значной логики // Тр. VII Междунар. конф. "Дискретные модели в теории управляющих систем" (Покровское, 4–6 марта 2006 г.). — М.: МАКС Пресс, 2006. — С. 107–113.

49. Дудакова О. С. О классах функций k-значной логики, монотонных относительно множеств ширины два // Вестн. Моск. ун-та. Серия 1. Матем. Механ. — 2008. — № 1. — С. 31–37.

50. Дудакова О. С. О конечной порожденности предполных классов монотонных функций многозначной логики // Математические вопросы кибернетики. Вып.17. — М.: Физматлит, 2008. — С. 13–104.

51. Дудакова О. С. Об одном семействе предполных классов функций k-значной логики, не имеющих конечного базиса // Вестн. Моск. ун-та. Серия 1. Матем. Механ. — 2006. — № 2. — С. 29–33.

52. Дудакова О. С. О конечной порожденности замкнутых классов монотонных функций в P_k // Ученые записки Казанского ун-та. Серия Физ.-матем. науки. — 2009. — Т. 151, кн. 2. — С. 65–71.

53. Burosch G. Über die Ordnung der prëvollständigen Klassen in Algebren von Prädikaten. — Preprint, WPU Rostock. — 1973.

54. Grünwald N. Bestimmung sämtlicher abgeschlossener Mengen aus $P_{3,2}$, deren Projektion F_8^n ist // Rostock, Math. Kolloq. — 1983. — 23. — S. 5–26.

55. Grünwald N. Beschreibung aller abgeschlossenen Mengen aus $P_{3,2}$, deren Projektion F_8^n ist, mit Hilfe von Relationen // Rostock, Math. Kolloq. — 1983. — 23. — S. 27–34.

56. Burosch G., Dassow J., Harnaw W., Lau, D. On subalgebras of an algebra of predicates // J. Inform. Process Cybern. EIK. — 1985. — V. 21, 1/2. — P. 9–22.

57. Lau D. Über abgeschlossene Teilmengen von $P_{k,2}$ // J. Inform. Process Cybern. EIK. — 1988. — 24, № 10. — S. 495–513.

58. Lau D. Über abgeschlossene Teilmengen von $P_{3,2}$ // J. Inform. Process Cybern. EIK. — 1988. — 24, № 11/12. — S. 561–572.

59. Михайлович А. В. О замкнутых классах трёхзначной логики, порожденных симметрическими функциями // Вестн. Моск. ун-та. Серия 1. Матем. Механ. — 2008. — № 4. — С. — 54–57.

60. Михайлович А. В. О классах функций трёхзначной логики, порожденных монотонными симметрическими функциями // Вестн. Моск. ун-та. Серия 1. Матем. Механ. — 2009. — № 1. — С. 33–37.

61. Михайлович А. В. О замкнутых классах функций многозначной логики, порожденных симметрическими функциями: Дис. ... канд. физ.-мат. наук. — М.: МГУ им. М. В. Ломоносова, 2009.

62. Биркгоф Г. Теория решеток. — М.: Наука, 1984.

63. Нгуен Ван Хоа. О структуре самодвойственных замкнутых классов трёхзначной логики в P_3 // Дискретная математика. — 1992. — Т. 4, вып 4. — С. 82–95.

64. Нгуен Ван Хоа. О семействах замкнутых классов k-значной логики, сохраняемых всеми автоморфизмами // Дискретная математика. — 1993. — Т. 5, вып 4. — С. 87–108.

65. Нгуен Ван Хоа. Описание замкнутых классов k-значной логики, сохраняемых всеми автоморфизмами // Докл. АН Беларуси. — 1994. — Т. 38, № 3. — С. 16–19.

66. Марченков С. С. Основные отношения S-классификации функций многозначной логики // Дискретная математика. — 1996. — Т. 8, вып 1. — С. 99–128.

67. Марченков С. С. S-классификация идемпотентных алгебр с конечными носителями // Докл. РАН. — 1996. — Т. 348, № 5. — С. 587–589.

68. Марченков С. С. S-классификация функций многозначной логики // Дискретная математика. — 1997. — Т. 9, вып 3. — С. 125–152.

69. Голунков Ю. В. Полнота систем функций в операторных алгоритмах, реализующих функции k-значной логики // Вероятностные методы и кибернетика. Вып. 17. — 1980. — С. 23–24.

70. Соловьев В. Д. Замкнутые классы в k-значной логике с операцией разветвления по предикатам // Дискретная математика. — 1990. — Т. 2, вып 4. — С. 18–25.

71. Тайманов В. А. О функциональных системах k-значной логики с операциями программного типа // Докл. АН СССР. — 1983. — Т. 268, № 6. — С. 1307–1310.

72. Тайманов В. А. Функциональные системы с операциями замыкания программного типа: Дис. ... канд. физ.-мат. наук. — М.: МГУ им. М. В. Ломоносова, 1983.

73. Kleitman D. On Dedekind's problem: the number of monotone Boolean functions // Proc. of the Amer. Math. Soc. — 1969. —Т. 21, № 3. — P. 677–682. [Рус. пер.: Клейтмен Д. О проблеме Дедекинда: число булевых монотонных функций // Кибернетический сб. Новая серия. Вып. 7. — 1970. — С. 43–52.]

74. Kleitman D., Markowsky G. On Dedekind's problem: the number of isotone Boolean functions, II // Trans. AMS. — 1975. — V. 213. — P. 373–390.

75. Угольников А. Б. О реализации монотонных функций схемами из функциональных элементов // Проблемы кибернетики. Вып. 31. — М.: Наука, 1976. — С. 167–185.

76. Угольников А. Б. О реализации функций из замкнутых классов схемами из функциональных элементов в полном базисе // ДАН СССР. — 1983. — Т. 271, № 1. — С. 49–51.

77. Угольников А. Б. О реализации функций из замкнутых классов схемами из функциональных элементов // Математические вопросы кибернетики. Вып. 1. — М.: Наука, 1988. — С. 89–113.

78. Тарасова О. С. Классы k-значной логики, замкнутые относительно расширенной операции суперпозиции // Вестн. Моск. ун-та. Серия 1. Матем. Механ. — 2001. — № 6. — С. 54–57.

79. Тарасова О. С. Классы функций k-значной логики, замкнутые относительно операций суперпозиции и перестановки // Математические вопросы кибернетики. Вып. 13. — 2004. — С. 59–112.

80. Тарасова О. С. Классы функций трёхзначной логики, замкнутые относительно операции суперпозиции и перестановки // Вестн. Моск. ун-та. Серия 1. Матем. Механ. — 2004. — № 1. — С. 25–29.

АНАЛИЗ И СИНТЕЗ АБСТРАКТНЫХ АВТОМАТОВ (КАЧЕСТВЕННЫЕ МЕТОДЫ)

В. Б. Кудрявцев (Москва)
И. С. Грунский, В. А. Козловский (Донецк)

В работе дан обзор ряда методов и результатов исследования задач поведенческой теории абстрактных конечных автоматов [1]. Классическими задачами этой теории являются задачи анализа процессов преобразования информации, осуществляемых автоматами, и свойств автоматов (прямые задачи), и задачи синтеза автоматов с заданными свойствами и идентификации (восстановления, распознавания, расшифровки, контроля и диагностики) автомата путем эксперимента с ним (обратные задачи). Как и во многих других теориях, обратные задачи обычно сложнее прямых. Это показывает, например, фундаментальная теорема теории конечных автоматов — теорема Клини, доказательство которой демонстрирует, что синтез (детерминированного) автомата по регулярному выражению сложнее задачи анализа автомата — построения по нему регулярного выражения, описывающего представленный в автомате язык. Еще более выпукло это было проявлено в основополагающей работе Э. Мура по теории экспериментов с автоматами [2], где впервые были рассмотрены задачи восстановления автомата по вход-выходным последовательностям как результату экспериментов. Заметим, что

задачи аналогичные задачам восстановления автоматов возникают и в прикладных областях, таких как диагностика вычислительной аппаратуры, а в последние годы в области формальных методов синтеза и верификации программно-аппаратных систем [3]. Важную роль при этом играют средства спецификации, и развитию этих средств уделяется большое внимание.

С этой точки зрения задача синтеза состоит в построении автомата по заданной его спецификации — заданию на необходимое, возможное и запрещенное поведение, а задача идентификации — в построении автомата, проводя эксперименты с заданным "черным ящиком" — реализацией этого автомата. В процессе эксперимента возникают фрагменты разрешенного и/или (ко)фрагменты запрещенного поведения автомата [4]. Фрагменты и кофрагменты являются дескрипторами автомата и образуют единую основу для решения задачи синтеза и идентификации с заданной точностью. Эта задача, в первую очередь, и рассматривается в работе.

Под экспериментом с автоматом понимается процесс подачи на автомат последовательности входных сигналов, наблюдение соответствующего поведения автомата и вывод заключений о функционировании и свойствах автомата, основанных на этих наблюдениях и априорной информации об автомате. Основная задача теории экспериментов состоит в разработке эффективных экспериментов, позволяющих получить определенные сведения о строении автомата, его функциях. При этом возникает большой круг задач, связанных с классификацией экспериментов, с вопросами разрешимости задач распознавания тех или иных свойств автомата определенными видами экспериментами, с оценками сложности минимальных экспериментов, достаточных для решения тех или иных задач распознавания, а также с оценками сложности построения этих экспериментов. Расширение понятия эксперимента приводит к понятию фрагмента и представления автомата, как более общих видов дескрипторов автоматов. При исследовании точности описания автомата фрагментами важную роль играют так называемые идентификаторы свойств автомата (состояний, входов, выходов) [4] — фрагменты, позволяющие однозначно идентифицировать эти свойства. Идентификаторы дают еще один пример дескриптора.

Таким образом, при исследовании задач синтеза/идентификации автоматов возник и интенсивно используется ряд частных видов дескрипторов автомата, и эти дескрипторы изучаются своими особыми методами. В связи с этим появляется необходимость создания общих методов изучения, создания и использования дескрипторов автомата при решении задач синтеза и идентификации автомата. При этом в качестве основного модельного дескриптора выступает фрагмент автомата. Анализ таких дескрипторов естественным

образом приводит еще к одному виду дескрипторов — системам определяющих соотношений.

В работе Мура [2] уже фактически затрагивались три основных аспекта теории экспериментов с автоматами: дескриптивный, сложностной, алгоритмический, касающиеся экспериментов как по распознаванию состояний автоматов, так и по распознаванию собственно автоматов, в первую очередь рассматриваемых в данной работе.

Следующие принципиальные шаги были сделаны Ф. Хенни [5], а затем М. П. Василевским [6]. Они проводили построение контрольных экспериментов путем специального размещения во входные последовательности специальных подпоследовательностей (диагностических, установочных, локализующих, характеристических и т. п.), по реакции на которые исследуемого автомата можно идентифицировать его внутренние состояния. В дальнейших исследованиях рассматривались различные виды таких последовательностей и способы их размещения в эксперименте [7]. Анализ этих последовательностей привел к понятию идентификатора состояния, введенному одним из авторов работы. На этом этапе получено большое количество частных способов построения контрольных и распознающих экспериментов для случаев, когда они заведомо существуют. Не исследованными остались условия существования и структура таких экспериментов в общем случае. Центральным и очень трудным оказался вопрос: что должно присутствовать в этих экспериментах, а что является издержками алгоритмов их построения, т. е. вопрос характеризации вышеуказанных экспериментов.

В работе дан обзор методов и некоторых базовых результатов в указанном направлении, полученных авторами и их учениками.

Структура основной части работы следующая. Одним из основных видов дескрипций автоматов являются эксперименты и представления автоматов. Используя топологические и теоретико-графовые методы, рассмотрены условия существования экспериментов и однозначности описания автоматов экспериментами и представлениями, сложность экспериментов и представлений.

Далее вводятся и обсуждаются алгебраические дескрипции и связанные с ними вопросы: задание автоматов определяющими соотношениями; системы определяющих соотношений для частичных автоматов и обобщения определяющих соотношений введением в них неравенств и определяющих пар для групповых автоматов; метрические характеристики систем определяющих соотношений. На плодотворность выявления связей автоматов и алгебраических конструкций указывал еще В. М. Глушков, отмечая первую работу Ю. И. Соркина [8] по теории определяющих соотношений для автоматов.

Заключительный блок результатов касается взаимосвязи экспе-

риментов и определяющих соотношений. Рассмотрены так называемые размеченные эксперименты и их связь с системами определяющих соотношений. Для так называемых циклических экспериментов групповых автоматов дана характеризация через определяющие пары. Приведены точные оценки параметров таких экспериментов, показана их лакунарность.

Автоматы и контрольные эксперименты

Рассматриваются автоматы Мили $A= (S, X, Y, \delta, \lambda)$, где S, X, Y — множества состояний, входов и выходов соответственно, а δ, λ — функции переходов и выходов.

Пусть заданы автомат-эталон A и класс автоматов F. Контрольный эксперимент (КЭ) автомата A относительно класса F — такое множество W вход-выходных слов, порождаемых автоматом A в некотором его состоянии, которое не порождается никаким другим (не эквивалентным эталону) автоматом из класса F (возможно, бесконечного).

В [9] получены условия существования контрольных экспериментов. На множестве инициальных автоматов вводится бэровская метрика β: $\beta(A, B) = 0$, если $A = B$, и $\beta(A, B) = \frac{1}{k}$, если $L_A^k \neq L_B^k$ и $L_A^{k-1} = L_B^{k-1}$. Здесь L_A^k — множество вход-выходных слов длины k, порождаемых начальным состоянием автомата A.

Для бэровской метрики β и произвольных $F \subseteq A_I(U)$, $A \in A_I(U)$ справедлив следующий критерий существования контрольного эксперимента.

Теорема 1. *Равносильны утверждения:*

1. *Существует контрольный эксперимент автомата A относительно F.*

2. *Множество L_A^k является контрольным экспериментом относительно A и F для некоторого k.*

3. $O_{\frac{1}{k}}(A) \bigcap F \subseteq \{A\}$ *для некоторого* k.

4. $O_{\frac{1}{k}}(A) \bigcap F$ *— конечное множество для некоторого* k*;*

5. $A \notin \lim F$.

Этот критерий показывает, что в бэровской метрике β процесс вывода заключений в процессе экспериментирования сводится к проверке условия 3. Если класс F конечен, то существует верхняя оценка t числа состояний автоматов из $F \bigcup \{A\}$ и, поэтому L_A^{2t} является контрольным экспериментом. Для произвольного бесконечного класса F критерий не конструктивен, однако существуют бесконечные классы, для которых этот критерий конструктивен.

Фрагменты автомата

Частичный автомат R называется (непосредственным) фрагмен-

том автомата A, если существует гомоморфизм R в A. Ядром конечного фрагмента R назовем такой его подавтомат Q, для которого существует полный слабый гомоморфизм φ, причем $\varphi(R) = Q$, а всякий слабый эндоморфизм фрагмента Q в себя является полным автоморфизмом.

Теорема 2. *Для каждого конечного фрагмента существует единственное с точностью до изоморфизма ядро.*

Пусть R — некоторый фрагмент эталона A, и t — некоторое произвольное зафиксированное состояние фрагмента. Фрагмент с зафиксированным состоянием обозначим R_t. Фрагмент R_t назовем идентификатором состояния s эталона, если для любого слабого гомоморфизма φ фрагмента R в эталон A выполняется равенство $\varphi(t) = s$. Справедлив следующий критерий существования идентификаторов состояний [4].

Теорема 3. *Равносильны утверждения:*

1. *Существует окрестность состояния s, являющаяся его идентификатором.*

2. *(φ_s, λ_s) является идентификатором состояния s.*

3. *Существует идентификатор (V_1, V_2) состояния s, для которого $|V_1| + |V_2| \leq n - 1$ и высота $h(V_2) \leq 2^{2n}$.*

Характеризация представлений автоматов

Далее полагаем, что класс $F \subseteq F_n$ — n-плотный относительно A, т. е. в классе F содержится всякий автомат, полученный из A изменением хотя бы одного значения его функции выходов или переходов, $A \in F$ и R — фрагмент A. Фрагмент R называется представлением для (A, F), если из существования гомоморфизма φ из R в $B \in F$ следует эквивалентность A и B.

Отношение σ на множестве состояний фрагмента R называется верифицированным отношением совместимости, если для любой пары $(a, b) \in \sigma$ и гомоморфизма φ фрагмента R в $B \in F$ справедливо равенство $\varphi(a) = \varphi(b)$. Это отношение порождает некоторую минимальную по включению конгруэнцию на множестве состояний и определяет, таким образом, фактор-автомат $[R]_\sigma$, который назовем сверткой.

Отношение ρ на множестве состояний фрагмента R называется верифицированным отношением несовместимости, если для любой пары $(a, b) \in \rho$ и гомоморфизма φ фрагмента R в $B \in F$ справедливо неравенство $\varphi(a) \neq \varphi(b)$. Такое отношение определяет некоторый обыкновенный неорграф G(R,P), ассоциированный со сверткой $[R]_\sigma$, где $P = (\sigma, \rho)$ — верифицированная пара для (R, F). Показывается, что всякий обыкновенный неорграф является ассоциированным при

подходящем выборе R, F [4].

Теорема 4. *R — представление для (A, F) тогда и только тогда, когда существует такая верифицированная пара $P = (\sigma, \rho)$ для (R, F), что выполняются условия:*

1. *Существует гомоморфизм φ автомата R в эталон A.*
2. $\Phi^1(R) = \Phi^1(A)$;
3. *Граф $G(R, P)$ однозначно n-раскрашиваемый.*

Приведенные достаточные и необходимые условия для распознавания представлений постулируют только существование верифицированной пары. Для ряда классов: определенно-диагностируемых порядка 1 (ОД-1) автоматов, групповых, без потери информации (БПИ-) автоматов, локально порожденных автоматов, базиса локальной порождаемости, дается конструктивный способ построения таких верифицированных пар, позволяющий сводить задачу анализа фрагментов на свойство "быть представлением" к задаче раскраски некоторого графа. Это, в свою очередь, позволяет оценить сложность распознавания представлений в терминах теории NP-полноты.

Теорема 5. *Задача распознавания представлений ОД-1 автомата в случаях: n-полного класса, класса групповых автоматов, БПИ-автоматов, базиса локальной порождаемости, является NP-полной. Для случая локально определенного класса она является полиномиальной.*

Системы определяющих соотношений для автоматов

Еще одним типом дескрипторов являются системы определяющих соотношений (СОС). Первой работой в этом направлении была статья Ю. И. Соркина [8]. В [10] его идеи обобщаются и развиваются, а в [11] показана и изучена связь СОС с контрольными экспериментами и представлениями автоматов.

Так, в [10] найдена минимальная система определяющих соотношений κ_A, названная канонической и рассмотрена ее структура; предложена процедура сведения (редукции) любой конечной системы определяющих соотношений к канонической; найден критерий, при котором конечное бинарное отношение является системой определяющих соотношений для заданного автомата A без построения автомата; предложено решение проблемы изоморфизма для инициальных конечных автоматов без явного построения баз этих автоматов; показана связь класса систем определяющих соотношений для данного автомата с другими его свойствами (обходами)и предложены процедуры перехода от обхода к системе определяющих соотношений и наоборот; понятия и аппарат систем определяющих соотношений распространяются на частичные автоматы. Исследо-

вание частичных автоматов происходит с помощью определяющей системы.

Приведем один из основных результатов, указывающий оценки параметров минимальных СОС. Пусть ρ — некоторое бинарное отношение на X^*. Это отношение назовем системой определяющих соотношений (СОС) для A, если $[\rho] = \rho_A$, где $[\rho]$ — правоконгруэнтное замыкание ρ, то есть наименьшая правая конгруэнция, содержащая ρ.

Пусть κ_A — произвольная каноническая СОС для автомата $A = (A, X, \delta_A, a_0)$, у которого $|X| = m$ и $|A| = n$, $N(\kappa_A)$ — число канонических систем.

Теорема 6. *Справедливы следующие оценки:*

1) $1 \le N(\kappa_A) \le m!$, *причем эти оценки достижимы для всех* m;

2) $|\kappa_A| = (m-1)n + 1$;

3) $S(\kappa_A) \ge \left(\frac{m^{l+1}-1}{m-1} - n\right) l + \left(m^l + n - \frac{m^{l+1}-1}{m-1}\right) m\,(l+1)$, *где* $l = \lceil \log_m n(m-1) + 1 \rceil - 1$;

4) $S(\kappa_A) \le n(m-1)(n-1) + m(2n-1)$, *причем эти оценки достижимы для всех* $n, m > 1$.

В работе [11] изучена связь контрольных экспериментов и представлений с СОС. При этом оказалось возможным рассматривать представления и КЭ относительно бесконечных классов автоматов. Контрольные эксперименты с автоматами относительно бесконечных классов существуют только при дополнительных допущениях о возможности наблюдения в эксперименте некоторой информации о внутренних состояниях исследуемого автомата. Было введено понятие размеченного эксперимента, расширяющее понятие эксперимента введением дополнительных средств наблюдения. Такие средства задаются специальными метками, наблюдаемыми в эксперименте и сигнализирующими о нахождении автомата в некоторых его состояниях. В частности, в качестве таких средств могут выступать идентификаторы состояний автомата. Такие эксперименты были детально изучены для случая групповых автоматов. Было предложено описание автоматов в виде так называемых определяющих пар в виде некоторой системы определяющих соотношений и порождающих специальной подгруппы свободной группы, определенной входным алфавитом автомата; найдены характеризации контрольных экспериментов группового автомата относительно бесконечного класса приведенных групповых автоматов; получены точные длины таких экспериментов при минимальных допущениях о средствах наблюдения. Увеличение мощности множества наблюдаемых в размеченном эксперименте меток расширяет возможности экспериментатора и может приводить к более эффективным по длине экспериментам.

Зафиксируем некоторое множество M меток мощности k. Пусть $w = (p, q) \in \lambda_t$, где t — состояние некоторого автомата B. Пусть

также $p = p_0p_1p_2...p_{k+1}$, $q = q_0q_1q_2...q_{k+1}$, где $\delta(t, p_0) = s_1$, $\delta(s_1, p_1) = s_2$, ..., $\delta(s_k, p_k) = s_{k+1}$, $\lambda(t, p_0) = q_0$, $\lambda(s_1, p_1) = q_1$, ..., $\lambda(s_k, p_k) = q_{k+1}$, и p_i непустое слово при $i = 1$, ..., k. Функцию φ , сопоставляющую каждому состоянию автомата некоторую метку или пустой символ e, назовем функцией разметки автомата B. Состояние $s \in S_B$, для которого $\varphi(s) \neq e$, назовем отмеченным. Тогда размеченным словом (размеченным экспериментом) называется слово $w_\varphi = (p_0, q_0)$ $\varphi(s_1)$ $(p_1, q_1)\varphi(s_2)$ ... $\varphi(s_k)(p_k, q_k)$ $\varphi(s_{k+1})(p_{k+1}, q_{k+1})$, если s_i — отмеченное состояние, $i = 1, ..., k+1$. Если $\varphi(s_i) = e$, то символ e в слове w_φ не указывается. Множество всевозможных размеченных экспериментов автомата B обозначим Φ_B.

Пусть F — некоторое подмножество полностью определенных сильно связных приведенных автоматов и $A \in F$ — эталон. Размеченный эксперимент $w_\varphi \in \Phi_A$ назовем контрольным размеченным экспериментом для A и F , если из принадлежности $w_\varphi \in \Phi_B$ для $B \in F$ следует изоморфизм автоматов A и B. Контрольный эксперимент с одной меткой назовем циклическим (КЦЭ).

Рассматриваются эксперименты для автоматов $A \in K_{n,m}$ и бесконечного класса $F(X, Y)$ приведенных групповых автоматов, где $K_{n,m} \subset F(X, Y)$ класс групповых автоматов с n состояниями и m входными символами. При этом рассматриваются приведенные контрольные эксперименты, то есть такие эксперименты, удаление любого слова из которых приводит к эксперименту, не являющемуся контрольным.

Пусть $d^A_{\min}$ — минимальная длина КЦЭ автомата A в алфавите $\bar{X}$, являющемся пополнением входного алфавита символами обратных элементов.

Теорема 7. 1. *Кратность приведенного КЦЭ равна* $mn - n + 1$.

2. *Для любого* $A \in K_{n,m} \subseteq F(X, Y)$ *справедливы неравенства:* $k((2m+1)(2m-1)^k - \frac{mn-n+1}{m}) + (k+1)(\frac{mn-n+1}{m} - (2m-1)^k)(2m-1) + mn - n + 1 \leq d^A_{\min} \leq n \cdot (mn - n + 1)$, *где* $k = [\log_{2m-1} \frac{mn-n+1}{m}]$, *причем обе оценки достижимы.*

Пусть $d' = k((2m+1)(2m-1)^k - \frac{mn-n+1}{m}) + (\frac{mn-n+1}{m} - (2m-1)^k)(2m-1)(k+1) + mn - n + 1$, $d'' = n \cdot (mn - n + 1)$.

Теорема 8. 1. *Для любого* $C = d'' - c \cdot (2m-2)$, $c \geq 0$, $C \geq d'$, *существует такой автомат* $A_i \in K_{n,m}$, *что* $d^{A_i}_{\min} = C$,

2. *Для любого* $C' \neq C$, $d' < C' < d''$, *не существует такого автомата* $A \in K_{n,m}$, *что* $d^A_{\min} = C'$.

Теоремы 7, 8 дают полное описание спектра возможных изменений длины минимальных КЦЭ групповых автоматов в расширенном

входном алфавите. Подобные точные лакунарные оценки получены и в случае обычного (не пополненного обратными элементами) входного алфавита.

На основе найденных оценок для размеченных экспериментов могут быть получены оценки длины минимальных контрольных экспериментов, понимаемых обычным образом. Например, в случае двух меток можно рассматривать автомат-эталон с двумя простыми начальными идентификаторами, максимальная длина которых не превосходит некоторой величины r. Тогда оценка длины контрольных экспериментов в таком случае по сравнению с приведенной оценкой для контрольного размеченного эксперимента увеличивается на сумму длины слов, необходимых для верификации идентификаторов, и суммарной длины идентификаторов, заменяющих метки соответствующих контрольных размеченных экспериментов.

В заключение заметим, что в коротком обзоре нет возможности во всей полноте отразить все ключевые моменты исследований, но даже приведенные понятия и утверждения говорят о рассматриваемой области исследований как сложившейся теории с нетривиальными результатами и актуальной с прикладной точки зрения. Бурное развитие формальных методов разработки, верификации и сопровождения программно-аппаратных систем вызвало к жизни целый ряд автоматоподобных, графовых и алгебраических моделей, на которые могут быть распространены результаты теории, фрагменты которой представлены в данной работе.

Список литературы

1. Кудрявцев В. Б., Алешин С. В., Подколзин А. С. Введение в теорию автоматов. — М.: Наука, 1985.

2. Мур Э. Ф. Умозрительные эксперименты с последовательностными машинами // Автоматы. — М.: ИЛ, 1956. — С. 179–210.

3. Крывый С. А., Матвеева Л. Е. Формальные методы анализа свойств систем // Кибернетика и системный анализ. —2003. — № 2. — С. 15–36.

4. Грунский И. С., Козловский В. А. Синтез и идентификация автоматов. — Киев: Наук. думка, 2004.

5. Hennie F. C. Fault detecting experiments for sequential circuits // Proc. 5 Annual Symp. "Switch. Circuits Th.and Logic. Design". — 1964. — P. 95–110.

6. Василевский М. П. О распознавании неисправностей автомата //Кибернетика. — 1973. — № 4. — С. 93–108.

7. Bhattacharyya A. Checking experiments on sequential machines. — New York: J. Wiley and Sons, 1989.

8. Соркин Ю. И. Теория определяющих соотношений для автоматов // Проблемы кибернетики. Вып. 9. — 1961. — С. 45–69.

9. Максименко И. К. Эксперименты в финитно-определенных метрических пространствах автоматов: Автореферат дис. ... канд. физ.-мат. наук. — Саратов: СГУ, 2000.

10. Сенченко А. С. Представление автоматов определяющими соотношениями их поведения: Автореферат дис. ... канд. физ.-мат. наук. — Киев: ИК НАН Украины, 2005.

11. Мучникова Л. А. Контрольные эксперименты с групповыми автоматами: Автореф. дис. ... канд. физ–мат.наук. — Киев: ИК НАН Украины, 2006.

КЛАССИФИКАЦИЯ АВТОМАТНЫХ БАЗИСОВ ПОСТА ПО РАЗРЕШИМОСТИ СВОЙСТВ ПОЛНОТЫ И А-ПОЛНОТЫ

Д. Н. Бабин (Москва)

Первый толчок к возникновению теории автоматов дала работа Э. Поста 1921 года [1]. В ней были получены фундаментальные результаты о строении решетки замкнутых классов булевых функций, которые были в дальнейшем методически переработаны и упрощены в книге С. В. Яблонского, Г. П. Гаврилова, В. Б. Кудрявцева [2]. Последующие работы по изучению алгебр автоматов велись под большим влиянием известных статей А. В. Кузнецова [3] и С. В. Яблонского [4] по теории функций k-значной логики.

Функции k-значной логики P_k могут рассматриваться как автоматы без памяти, к которым применяются операции суперпозиции. Основу результатов для функций из P_k составляет подход, опирающийся на понятие предполного класса. На этом пути С.В. Яблонским путем явного описания всех предполных классов была решена задача о полноте для функций трехзначной логики. После усилий многих исследователей при $k > 3$ в P_k были описаны все семейства предполных классов. Заключительные построения в этой задаче провел Розенберг [5].

Одновременно с изучением функций без памяти (без учета времени), были сделаны попытки применения аппарата предполных классов в задаче полноты для автоматов. В. Б. Кудрявцев получил фундаментальный результат негативного характера, который показал континуальность множества предполных классов автоматных функций [6]. В дальнейшем, М. И. Кратко была показана алгоритмическая неразрешимость задачи о полноте для автоматных функций [7].

Еще в 1961 г. А. А. Летичевским [8] был получен алгоритм решения задачи о полноте для конечных систем автоматов, выдающих номер своего состояния (автоматы Медведева), при наличии в исследуемой системе всех булевых функций. В 1986 г. В. А. Буевич [9] показал алгоритмическую разрешимость задачи A-полноты для конечных систем автоматов, содержащих все булевы функции. В 1992 г. автор [10] показал, что существует алгоритм распознавания полноты при наличии в рассматриваемой системе автоматов всех булевых функций.

В этой ситуации интересно использовать разрешимость автоматной полноты как инструмент для исследования базисов функций, а именно, исследовать на полноту (A-полноту) системы вида $\Phi \cup \nu$, где Φ — замкнутый класс функций из P_k (его конечный базис), а ν — конечная система автоматных функций.

В результате серии работ автора для P_2 была построена классификация замкнутых классов Поста по их способности в качестве добавки в произвольный автоматный базис обеспечивать алгоритмическую разрешимость полноты. Имеют место теоремы [11]:

Теорема 1. *Задача о полноте для систем автоматных функций вида* $\Phi \cup \nu$, *где* $\Phi \subseteq P_2$ — *фиксированный класс булевых функций, а* ν — *произвольная конечная система автоматных функций, алгоритмически разрешима точно тогда, когда* $\Phi \supseteq D_2$ *или* $\Phi \supseteq L_4$.

Теорема 2. *Задача об A-полноте для систем автоматных функций вида* $\Phi \cup \nu$, *где* $\Phi \subseteq P_2$ — *фиксированный класс булевых функций, а* ν — *произвольная конечная система автоматных функций, алгоритмически разрешима точно тогда, когда* $\Phi \supseteq D_2$ *или* $\Phi \supseteq L_4$.

Пусть M некоторое множество автоматных функций. Имеют место следствия из теорем 1, 2.

Следствие 1. *Задача о полноте для систем автоматных функций вида* $\Phi \cup \nu$, *где* $\Phi \subseteq P_2$ — *фиксированный класс булевых функций, а* ν — *произвольная конечная система автоматных функций из M, алгоритмически разрешима если* $\Phi \supseteq D_2$ *или* $\Phi \supseteq L_4$.

Следствие 2. *Задача об A-полноте для систем автоматных функций вида* $\Phi \cup \nu$, *где* $\Phi \subseteq P_2$ — *фиксированный класс булевых функций,а* ν — *произвольная конечная система автоматных функций из M, алгоритмически разрешима если* $\Phi \supseteq D_2$ *или* $\Phi \supseteq L_4$.

Построенная классификация продолжается на функции из P_k, $k > 2$, и уже на уровне максимальных (предполных) классов обнаружены противоположные случаи.

Список литературы

1. Post E. L. Two-valued iterative systems of mathematical logic //

Ann. Math. Stud. Princeton; London: Princeton Univ. Press, 1941. — № 5.

2. Яблонский С. В., Гаврилов Г. П., Кудрявцев В. Б. Функции алгебры логики и классы Поста. — М.: Наука 1966.

3. Кузнецов А. В. О проблемах тождества и функциональной полноты для алгебраических систем // Труды третьего всесоюзного математического съезда. Т. 2. — М.: Изд. АН СССР, 1956. — С. 145–146.

4. Яблонский С. В. Функциональные построения в k-значной логике // Труды Матем. ин-та им. В. А. Стеклова. — М.: Изд. АН СССР, 1958. — Т. 51. — С. 5–142.

5. Rosenberg I. La structure des fonctions de plusiers variables sur un ensemble fini // Comptes Rendus Acad. Sci. — Paris, 1965. — № 260. — С. 3817–3819.

6. Кудрявцев В. Б. О мощностях множеств предполных классов некоторых функциональных систем, связанных с автоматами // ДАН СССР. — 1963. — Т. 151, № 3. — С. 493–496.

7. Кратко М. И. Алгоритмическая неразрешимость проблемы распознавания полноты для конечных автоматов // ДАН СССР. — 1964. — Т. 155, № 1. — С. 35–37.

8. Летичевский А. А. Условия полноты для конечных автоматов // Вычислительная математика и математическая физика. — 1961. — № 4. — С. 702–710.

9. Буевич В. А. Условия А-полноты для автоматов. — М: Изд. МГУ, 1986.

10. Бабин Д. Н. Разрешимый случай задачи о полноте автоматных функций// Дискретная математика. — 1992. — Т. 4, вып. 4. — С. 41–56.

11. Бабин Д. Н. О классификации автоматных базисов Поста по разрешимости свойств полноты и А-полноты // Доклады Академии наук. — 1999. — Т. 367, № 4. — С. 439–441.

ВЫЧИСЛИТЕЛЬНЫЕ ВОЗМОЖНОСТИ КЛАССИЧЕСКИХ И КВАНТОВЫХ ВЕТВЯЩИХСЯ ПРОГРАММ

Ф. М. Аблаев (Казань)

Предварительные сведения. Исследования в области квантовых вычислений имеют два источника мотиваций. Технологический и собственно математический.

Эксперты в области электронных технологий прогнозируют, что к 2020 году производители электронных систем подойдут к уровню технологий 10 *нм* и менее. Это означает, что к 20-м годам на основе кремниевых соединений будут сконструированы транзисторы минимально возможных размеров. Дальнейшему уменьшению размеров объектов электронных технологий уже будет мешать эффект квантового туннелирования (эффект самопроизвольного порождения потока электронов между полюсами транзисторов).

Математические основания следующие. Естественным обобщением вероятностных автоматов являются линейные автоматы. Квантовые (один раз измеряемые) модели вычислений по сути — это специальные варианты линейных моделей вычислений. Часть результатов из теории вероятностных автоматов и машин естественным образом обобщается на случай квантовых моделей.

Теория квантовых вычислений опирается на постулаты квантовой механики. Пусть $\mathcal{H}^d$ — d-мерное гильбертово пространство. Для обозначения элементов пространства $\mathcal{H}^d$ принято использовать нотацию Дирака: $|\psi\rangle$ для вектора-столбца. Будем писать ψ, когда из контекста ясно, о чем идет речь.

Квантовый бит (*кубит*) является ключевым понятием теории квантовых вычислений. Математически кубит $|\psi\rangle$ — это комплекснозначный вектор пространства $\mathcal{H}^2$, т. е. $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, где векторы $|0\rangle$ и $|1\rangle$ образуют ортонормированный базис в $\mathcal{H}^2$, а комплексные числа α и β удовлетворяют условию $|\alpha|^2 + |\beta|^2 = 1$. Числа $|\alpha|^2$, $|\beta|^2$ — это вероятности обнаружить кубит ψ в состоянии 0 или 1 соответственно при измерении системы ψ.

Обозначим через $|i\rangle$ вектор из $\mathcal{H}^d$, у которого на i-й позиции 1, а все остальные компоненты нулевые. Эту систему $|1\rangle$, $\ldots$, $|d\rangle$ называют стандартным вычислительным базисом. Векторы стандартного базиса также представляют в виде $|00\ldots0\rangle$, $\ldots$, $|bin(i)\rangle$, $\ldots$, $|11\ldots1\rangle$, где $bin(i)$ — это двоичное представление числа i. Состояние $|\psi\rangle$ замкнутой системы, состоящей из n кубит, в общем случае задается единичным вектором в пространстве $\mathcal{H}^{2^n}$:

$$|\psi\rangle = \sum_{i=1}^{2^n} \alpha_i |i\rangle \qquad \text{или} \qquad |\psi\rangle = \sum_{\sigma\in\{0,1\}^n} \alpha_\sigma |\sigma\rangle,$$

где $\sum\limits_{i=1}^{2^n} |\alpha_i|^2 = 1$, $\sum\limits_{\sigma\in\{0,1\}^n} |\alpha_\sigma|^2 = 1$.

Пусть n кубит находятся в состояниях $|\psi_1\rangle, \ldots, |\psi_n\rangle$. Если состояние $|\psi\rangle$ квантовой системы может быть выражено через тензорное произведение состояний этих кубит $|\psi\rangle = |\psi_1\rangle \otimes \cdots \otimes |\psi_n\rangle$, то такое состояние называют разложимым. В то же время существуют так называемые *неразложимые или сцепленные состояния* квантовых регистров, которые не могут быть представлены тензорным произведением состояний отдельных кубит. Сцепленные состояния играют ключевую роль при разработке эффективных квантовых алгоритмов.

Динамика изменения состояния замкнутой квантовой системы описывается унитарными преобразованиями. Другими словами, состояние ψ_1 системы в момент времени t_1 связано с состоянием ψ_2 в момент времени t_2 следующим образом: $\psi_1 = U\psi_2$, где U — это унитарная $2^n \times 2^n$ матрица.

Детерминированные ветвящиеся программы (DBP) с одной стороны — частный случай контактных схем, с другой стороны, их можно рассматривать как машинную модель вычислений. Различные аспекты теории классических ветвящихся программ представлены в книге [2].

DBP над множеством переменных $X = \{x_1, \ldots, x_n\}$ — это ориентированный ациклический граф, вершины которого делятся на множество внутренних и множество финальных вершин. Финальные вершины не имеют исходящих ребер и помечены нулем или единицей соответственно. Каждой внутренней вершине v соответствует переменная $x \in X$, каждая внутренняя вершина имеет два исходящих ребра, помеченные 0 ($x = 0$) и 1 ($x = 1$), соответственно.

Для DBP P входной набор $\sigma \in \{0,1\}^n$ порождает путь из выделенной начальной вершины v_0 в финальную вершину (0 или 1). DBP P вычисляет функцию $f(X)$, если для всех $\sigma \in \{0,1\}^n$ значение функции $f(\sigma)$ совпадает со значением финальной вершины, достигаемой на наборе σ.

Сложность $S(P)$ программы P — это число ее внутренних вершин.

Нижние оценки сложности. Коммуникационный подход. Самая высокая нижняя оценка $\Omega(n^2/\log^2 n)$ представления булевой функции (варианта мультиплексорной функции) в ветвящихся программах доказана с применением метода Нечипорука (см., например, книгу [2]). Метод Нечипорука является коммуникационным методом доказательства нижних оценок и может быть сформулирован в следующем виде:

Пусть $S \subseteq X$, пусть $Z = X \backslash S$. Через π обозначим соответствующее разбиение множества X. Через $M^\pi(f)$ обозначим булеву

$2^{|Z|} \times 2^{|S|}$ матрицу (называемую коммуникационной матрицей функции $f(X)$), такую, что на пересечении строки, соответствующей набору σ (значений переменных из Z) и столбца, соответствующего набору γ (значений переменных из S) стоит значение $f(\sigma, \gamma)$.

Для разбиения π множества X односторонняя (одноразундовая) коммуникационная сложность $C_1^\pi(f)$ функции $f(X)$ определяется равенством $C_1^\pi(f) = \log nrow(M^\pi(f))$, где $nrow(M^\pi(f))$ — это число попарно различных строк матрицы $M^\pi(f)$. Коммуникационная форма нижней оценки Нечипорука следующая:

Пусть функция $f(X)$ зависит от всех аргументов существенным образом. Пусть $S_1, \ldots, S_k \subseteq X$ — попарно непересекающиеся множества, а $\pi_1, \ldots, \pi_k$ — соответствующие разбиения X. Тогда

$$S(f) = \Omega\left(\sum_{i=1}^{k} \frac{C_1^{\pi_i}(f)}{\log C_1^{\pi_i}(f)}\right).$$

DBP называется *уровневой*, если ее вершины могут быть разбиты на уровни $0, 1, \ldots$ таким образом, что для каждого i ребра из вершин уровня i ведут только в вершины уровня $(i+1)$. Уровневая DPB называется *забывающей*, если на каждом уровне читается только одна переменная. Пусть $width_i(P)$ — это число вершин DPB P на уровне i. Число

$$width(P) = \max_i width_i(P)$$

называется шириной DPB P. Ветвящаяся программа P называется *читающей один раз* (read-once), если на каждом пути каждая переменная $x \in X$ считывается ровно один раз. Для читающих один раз программ в 80-х годах были различными авторами доказаны экспоненциальные нижние оценки сложности реализации индивидуальных функций [2]. Упорядоченная ветвящаяся диаграмма решений (OBDD) — это, читающая один раз, забывающая ветвящаяся программа.

В случае OBDD коммуникационный подход дает следующую оценку:

Пусть детерминированная OBDD P вычисляет $f(X)$. Пусть π — разбиение множества X, определенное в соответствии с порядком τ считывания переменных в P. Тогда

$$width(P) = \Omega\left(2^{C_1^\pi(f)}\right).$$

Квантовая ветвящаяся программа (QBP) является обобщением забывающей DBP. Определения различных вариантов моделей квантовых ветвящихся программ даны в работе [1]. В работе [1] приводятся результаты нашей группы, полученные до 2004 года. Даются ссылки на оригинальные работы.

Для квантовых OBDD коммуникационная техника дает следующую нижнюю оценку:

Пусть квантовая OBDD Q вычисляет $f(X)$. Пусть π — разбиение множества X, определенное в соответствии с порядком τ считывания переменных в P. Тогда

$$width(Q) = \Omega\left(C_1^{\pi}(f)\right).$$

С помощью этой оценки доказывается нижняя оценка $\Omega(\log m)$ для ширины квантовой OBDD, вычисляющей функцию MOD_m. Функция MOD_m определяется условием: на наборе σ $MOD_m(\sigma) = 1$ тогда и только тогда, когда число единиц в наборе σ кратно m. Отметим, что любая детерминированная OBDD, вычисляющая MOD_m, должна иметь ширину не менее m.

Методы построения квантовых ветвящихся программ. В работе [1] приводится верхняя оценка $O(\log m)$ на ширину квантовой OBDD, вычисляющей функцию MOD_m, что доказывает достаточную степень точности нижней оценки для квантовых OBDD. Эти оценки (нижняя и верхняя оценка реализации MOD_m в квантовых OBDD) являются основными результатами диссертационной работы А. Гайнутдиновой 2004 года. Метод построения эффективных квантовых алгоритмов в терминах квантовых OBDD, предложенный в диссертационной работе А. Гайнутдиновой получил дальнейшее развитие в диссертационном исследовании А. Хасьянова. В результате были построены эффективные квантовые OBDD для целого ряда функций, в частности, для функции HSP, представляющей "булевский вариант" задачи "скрытая подгруппа". Эта задача является обобщением задачи факторизации числа.

В диссертационной работе А. Васильева разработанные ранее подходы построения эффективных квантовых OBDD обобщены в виде квантового "метода отпечатков" (fingerprinting method). Вероятностный "метод отпечатков" был предложен Р. Фрейвалдом в 1980-х годах для вероятностного распознавания равенства слов.

Метод отпечатков — это техника, позволяющая представлять объекты (слова в некотором конечном алфавите) их образами (*отпечатками, fingerprints*), значительно более компактными, чем оригиналы. Кроме того, она позволяет с высокой вероятностью извлекать информацию о входном наборе.

Ключевым моментом использования предложенного метода является представление вычисляемых булевых функций *характеристическими полиномами*. Назовем полином g_f над кольцом вычетов $\mathbf{Z}_m$ характеристическим для булевой функции $f(x_1, \ldots, x_n)$, если для любого $\sigma \in \{0,1\}^n$ выполняется: $f(\sigma) = 1 \iff g_f(\sigma) = 0$.

Техника отпечатков. Для решаемой задачи фиксируется допустимая вероятность ошибки $\epsilon \in (0,1)$ и выбирается характеристический полином g над кольцом $\mathbf{Z}_m$ (m выбирается подходящим способом).

Для входного набора $\sigma = (\sigma_1 \ldots \sigma_n)$ порождается его отпечаток $|h_\sigma\rangle$ (сцепленное состояние квантовой системы), соединяющий в себе t однокубитных отпечатков $|h^i_\sigma\rangle$:

$$\begin{aligned} |h^i_\sigma\rangle &= \cos\tfrac{2\pi k_i g(\sigma)}{m}|0\rangle + \sin\tfrac{2\pi k_i g(\sigma)}{m}|1\rangle, \\ |h_\sigma\rangle &= \tfrac{1}{\sqrt{t}}\sum_{i=1}^{t}|i\rangle|h^i_\sigma\rangle. \end{aligned}$$

Отметим, что, используя "максимальную" сцепленность состояния $|h_\sigma\rangle$ в нем можно представить информацию о t кубитах $|h^i_\sigma\rangle$. При формировании состояния $|h^i_\sigma\rangle$ при считывании σ последний из $\log t + 1$ кубитов состояния $|h^i_\sigma\rangle$ одновременно (*квантово параллельно*) поворачивается на t различных углов вокруг оси $\hat{y}$ сферы Блоха.

Целью таких преобразований является распознавание свойства: верно ли, что $g(\sigma) = 0$. Для этого параметры $k_i \in \{1, \ldots, m-1\}$ для всех $i = \overline{1,t}$ выбираются специальным образом, исходя из следующего определения.

Для числа $\epsilon \in (0,1)$ множество параметров $K = \{k_1, \ldots, k_t\}$ называется "хорошим" для целого числа $l \neq 0 \pmod m$, если

$$\frac{1}{t^2}\left(\sum_{i=1}^{t}\cos\frac{2\pi k_i l}{m}\right)^2 < \epsilon.$$

Неформально, такое множество гарантирует, что вероятность ошибки реализации функции $f(X)$, квантовой OBDD, реализованной квантовым методом отпечатков, будет ограничена константой ϵ.

Комбинаторные рассуждения показывают, что существует множество K, где $|K| = t$, которое является "хорошим" для всех целых $l \neq 0 \pmod m$.

Примеры. Квантовый метод отпечатков хорошо работает на функциях, в основе которых лежит проверка равенства.

- MOD'_m. Эта функция отличается от MOD_m тем, что входной набор интерпретируется как двоичное число.
- EQ_n. Функция EQ_n проверяет равенство двух n-битных двоичных наборов
- $Palindrome_n(x_1, \ldots, x_n) \equiv \left[x_1 x_2 \ldots x_{\lfloor n/2 \rfloor} = x_n x_{n-1} \ldots x_{\lceil n/2 \rceil + 1}\right]$.
- $PERM_n$. Эта функция проверяет, является ли булева $n \times n$ матрица перестановочной.

В таблице приводятся нижние оценки сложности (ширины) реализации перечисленных функций в детерминированных и квантовых OBDD, полученные коммуникационным методом. Приводятся также верхние оценки реализации этих функций в квантовых OBDD, получаемые квантовым методом отпечатков. Полученные верхние и нижние оценки достаточно точны.

	OBDD	QOBDD
	ниж. оц.	ниж. оц., верх. оц.
MOD_m	$\Omega(m)$	$\Omega(\log m)$, $O(\log m)$
MOD'_m	$\Omega(m)$	$\Omega(\log m)$, $O(\log m)$
EQ_n	$2^{\Omega(n)}$	$\Omega(n)$, $O(n)$
$Palindrome_n$	$2^{\Omega(n)}$	$\Omega(n)$, $O(n)$
$PERM_n$	$\Omega(2^n n^{-1/2})$	$\Omega(n)$, $O(n \log n)$

Заключение. Отметим, что квантовый метод отпечатков претерпел значительные изменения по сравнению со своим "классическим вероятностным родителем". Дополнительным условием при разработке квантового варианта метода отпечатков было требование его реализуемости в модели квантовой OBDD. Модель OBDD с классической токи зрения достаточно слабая модель вычислений. Однако при построении квантовых (пока чисто математических) моделей вычислений нужно учитывать, что разрабатываемые квантовые технологии еще в зачаточном состоянии и в первую очередь нужно изучить наипростейшие варианты моделей для реализации квантовых алгоритмов.

Работа выполнена при финансовой поддержке РФФИ, проекты 08-07-00449-а и 09-01-97004-р-поволжье-а.

Список литературы

1. Аблаев Ф.М. О сложности классических и квантовых моделей вычислений // Математические вопросы кибернетики. Вып. 13. — 2004. — С. 137–146.

2. Wegener I. Branching programs and binary decision diagrams // SIAM Monographs on Discrete Mathematics and Applications, 2000.

ЭЛЕМЕНТЫ ТЕОРИИ НЕДООПРЕДЕЛЕННОЙ ИНФОРМАЦИИ

Л. А. Шоломов (Москва)

С недоопределенными данными имеют дело во многих задачах информатики. Поэтому целесообразно изучать такие данные в качестве самостоятельного объекта подобно тому, как это делается в теории информации для полностью определенных данных. Приведем некоторые результаты в этом направлении. Их развернутое изложение имеется в [4–7].

Задан алфавит $A_0 = \{a_0, a_1, \ldots, a_{m-1}\}$ *основных символов*. Пусть $M = \{0, 1, \ldots, m-1\}$ и каждому (непустому) $T \subseteq M$ сопоставлен символ a_T. Символы алфавита $A = \{a_T,\, T \subseteq M\}$ называются *недоопределенными* и *доопределением* символа $a_T \in A$ считается всякий основной символ a_i, $i \in T$, а доопределением последовательности в алфавите A — любая последовательность, полученная из нее заменой всех символов доопределениями. Символ a_M, доопределимый любым основным символом, называется *неопределенным* и обозначается $*$.

Пусть имеется источник X, порождающий символы $a_T \in A$ независимо с вероятностями p_T. Такой источник будем называть *недоопределенным*, при выполнении условия $p_T = 0$ для $a_T \notin A_0$ — *полностью определенным*, а в случае $p_T = 0$ для $a_T \notin A_0 \cup \{*\}$ — *частично определенным*. *Энтропией источника* X назовем величину

$$\mathcal{H}(X) = \min_Q \Big\{ - \sum_{T \subseteq M} p_T \log \sum_{i \in T} q_i \Big\}, \tag{1}$$

где $\log x = \log_2 x$, минимум берется по наборам $Q = (q_i,\ i \in M)$, $q_i \geq 0$, $\sum_{i \in M} q_i = 1$. Если набор $\hat{Q}$ минимизирует правую часть, будем говорить, что на нем достигается энтропия.

Нетрудно показать, что для всюду определенного источника X величина $\mathcal{H}(X)$ совпадает с энтропией Шеннона. Для частично определенного источника она задается выражением

$$\mathcal{H}(X) = (1 - p_*)\log(1 - p_*) - \sum_{0 \le i \le m-1} p_i \log p_i.$$

Приведем некоторые свойства энтропии $\mathcal{H}(X)$ и сравним их со свойствами энтропии Шеннона $H(X)$ [1].

1°. $\mathcal{H}(X) \ge 0$, *причем* $\mathcal{H}(X) = 0 \Leftrightarrow \bigcap_{T:\, p_T > 0} T \ne \emptyset$.

Это означает, что $\mathcal{H}(X) = 0$ лишь если X порождает последовательности, доопределимые одинаковыми символами. Для полностью определенного источника равенство $H(X) = 0$ имеет место лишь если X порождает последовательности одинаковых символов.

2° $\mathcal{H}(X) \le \log m - \sum\limits_{1 \le t \le m} p(t) \log t$, *где* $p(t) = \sum\limits_{T:\, |T| = t} p_T$, $1 \le t \le m$, — *распределение числа* t *доопределений символов источника* X.

Если X полностью определен, то $p(t) = 0$ для $t \ge 2$, и это неравенство превращается в известное соотношение $H(X) \le \log m$.

3°. $\mathcal{H}(XY) \le \mathcal{H}(X) + \mathcal{H}(Y)$, *а если* X *и* Y *статистически независимы, имеет место равенство.*

В отличие от обычной энтропии H, независимость здесь не является необходимой для равенства. Если X и Y — частично определены, то множество совместных распределений P_{XY}, для которых справедливо равенство, образуют выпуклый многогранник размерности $|A||B| - |A_0||B_0|$, где алфавиты A, A_0 и B, B_0 относятся к источникам X и Y. Поскольку для всюду определенных источников выполнено $A = A_0$ и $B = B_0$, многогранник вырождается в точку и условие независимости становится также необходимым.

Задача кодирования недоопределенных источников отличается от обычной задачи кодирования источников тем, что по коду последовательности следует восстановить какое-либо ее доопределение. Качество кодирования характеризуется *средней длиной кода* $\bar{l}$ на символ последовательности. Теорема кодирования полностью определенных источников обобщается на недоопределенный случай.

4°. *При любом способе кодирования недоопределенного источника* X *выполнено* $\bar{l} \ge \mathcal{H}(S)$ *и существует кодирование, для которого* $\bar{l} \le \mathcal{H}(S) + o(1)$.

Для набора натуральных чисел $\mathbf{l} = (l_T,\ T \subseteq M)$, $\sum_T l_T = n$, обозначим через $\mathcal{K}_n(\mathbf{l})$ множество всех последовательностей длины

n в алфавите A, в которых символ a_T, $T \subseteq M$, встречается l_T раз. Обозначим через $N_n(\mathbf{l})$ минимальную мощность множества последовательностей в алфавите A_0, содержащего доопределение каждой последовательности из $\mathcal{K}_n(\mathbf{l})$. Величину $\log N_n(\mathbf{l})$ назовем *комбинаторной энтропией* класса $\mathcal{K}_n(\mathbf{l})$.

5°. *Справедливы оценки комбинаторной энтропии*

$$n\mathcal{H}(\mathbf{l}/n) - c\log n \le \log N_n(\mathbf{l}) \le n\mathcal{H}(\mathbf{l}/n) + c\log n,$$

где $c = c(m)$ *— некоторая константа.*

Из них следует, что энтропия (1) согласована с алгоритмической интерпретацией энтропии в терминах сложности [2].

Приведем некоторые результаты, не имеющие аналогов в классической теории информации, поскольку связаны с наличием неопределенных символов. Пусть $\mathcal{K}_n(l)$, $l \le n$, — класс всех последовательностей длины n с l булевыми символами и $n-l$ неопределенными символами $*$, $\log N_n(l)$ — его комбинаторная энтропия. Э. И. Нечипорук [3] доказал, что $\log N_n(l) = l + O(\log n)$. Этот факт допускают следующую интерпретацию, которую будем называть *эффектом Нечипорука.* Недоопределенные последовательности и последовательности меньшей длины, полученные из них удалением неопределенных символов, могут быть представлены кодами одинаковой с точностью до $O(\log n)$ длины.

Этот эффект обобщается для недоопределенные последовательностей общего вида.

6°. *Если класс* $\mathcal{K}_{n'}(\mathbf{l}')$, $n' = n - l_*$, *образован из класса* $\mathcal{K}_n(\mathbf{l})$ *удалением в его последовательностях символов* $*$, *то*

$$\log N_n(\mathbf{l}) = \log N_{n'}(\mathbf{l}') + O(\log n).$$

Эффект Нечипорука распространяется и на кодирование с заданным критерием верности. Пусть последовательности в конечном алфавите $B = \{b_i,\ i \in I\}$ должны быть представлены последовательностями (той же длины n) в конечном алфавите $D = \{d_j,\ j \in J\}$ при выполненении некоторых условий верности воспроизведения. Будем считать, что эти условия задаются отношением $\mathbf{b}\omega\mathbf{d}$ допустимости воспроизведения $\mathbf{d}$ вместо $\mathbf{b}$. Будем полагать, что отношение ω не зависит от нумерации разрядов последовательностей. Символ алфавита B будем называть *неопределенным* (*для* ω) и обозначать $*$, если для любых $\mathbf{b}$, $\mathbf{d}$ и $\hat{\mathbf{d}}$ таких, что $\hat{\mathbf{d}}$ и $\mathbf{d}$ отличаются лишь в разрядах, где $\mathbf{b}$ содержит символ $*$, выполнено $\mathbf{b}\omega\mathbf{d} \Leftrightarrow \mathbf{b}\omega\hat{\mathbf{d}}$.

Пусть $\mathcal{K}_n(\mathbf{l})$, $\mathbf{l} = (l_i,\ i \in I)$, $\sum_i l_i = n$, — класс последовательностей длины n в алфавите B, в которых символ b_i, $i \in I$, встречается l_i раз, а $N_{n,\omega}(\mathbf{l})$ — минимальное число последовательностей в алфавите D, содержащих для каждой последовательности из $\mathcal{K}_n(\mathbf{l})$ ω-допустимую. Величину $\log N_{n,\omega}(\mathbf{l})$ назовем *комбинаторной ω-энтропией* класса $\mathcal{K}_n(\mathbf{l})$. Применительно к ω-энтропии эффект Нечипорука формулируется в следующем виде.

7°. *Если класс $\mathcal{K}_{n'}(\mathbf{l}')$, $n' = n - l_*$, образован из $\mathcal{K}_n(\mathbf{l})$ удалением в его последовательностях символов $*$ и отношение допустимости ω' для $\mathcal{K}_{n'}(\mathbf{l}')$ индуцировано отношением ω для $\mathcal{K}_n(\mathbf{l})$, то*

$$\log N_{n,\omega}(\mathbf{l}) = \log N_{n',\omega'}(\mathbf{l}') + O(\log n).$$

Доопределение $\dot{X}$ источника X представляет собой полностью определенный источник, который строится по X применением некоторого набора переходных вероятностей $p_{i|T} = p(a_i|a_T)$, $i \in M$, $T \subseteq M$, и порождает символы a_i с вероятностями $\dot{p}_i = \sum_T p_T p_{i|T}$. Обычным образом вводится взаимная информация [1]

$$I(X, \dot{X}) = \sum_{T,i} p_T p_{i|T} \log \frac{p_{i|T}}{\dot{p}_i}.$$

Справедливо следующее утверждение.

8°. *Для любого доопределения $\dot{X}$ выполнено $I(X, \dot{X}) \geq \mathcal{H}(X)$ и существует доопределение $\hat{X}$, для которого $I(X, \hat{X}) = \mathcal{H}(X)$.*

Доопределение $\hat{X}$ называется *лучшим* (о его сложностной интерпретации см. в секционном докладе автора на этой конференции). Дальше понадобятся параметры лучшего доопределения.

9°. *Доопределение $\hat{X}$ является лучшим тогда и только тогда, когда оно задается переходными вероятностями $p_{i|T} = \hat{q}_i \Big/ \sum_{j \in T} \hat{q}_j$, где $\hat{Q} = (\hat{q}_i,\ i \in M)$ — один из наборов, на которых достигается энтропия $\mathcal{H}(X)$.*

При весьма слабых условиях энтропия достигается в единственной точке и лучшее доопределение единственно.

Перейдем к мере информации недоопределенных данных. С учетом обычного соотношения

$$\mathcal{I}(X, Y) = \mathcal{H}(Y) - \mathcal{H}(Y|X),$$

связывающего меру информации в X относительно Y с условной энтропией $\mathcal{H}(Y|X)$, введение меры информации недоопределенных данных сводится к определению для них понятия условной энтропии. Существенную роль в классической теории инфомации играет правило сложения энтропий $H(X) + H(Y|X) = H(XY)$. Вариант этого правила включен Шенноном в число свойств, аксиоматически задающих энтропию, и во многом определил вид энтропийной функции. При введении условной энтропии $\mathcal{H}(Y|X)$ для недоопределенных данных этому свойству будем уделять особое внимание.

Пусть произведение XY недоопределенных источников с алфавитами $A = \{a_T,\, T \subseteq M\}$ и $B = \{b_U,\, U \subseteq L\}$, задано совместным распределением $p_{TU} = p(a_T, b_U)$, $T \subseteq M$, $U \subseteq L$.

Будем считать вначале, что X полностью определен. Тогда условную энтропию введем равенством [1] $\mathcal{H}(Y|X) = \sum_i p(a_i)\mathcal{H}(Y|a_i)$. Величины $\mathcal{H}(Y|a_i)$ находятся подобно (1) с заменой вероятностей условными вероятностями $p_{U|i} = p(b_U|a_i)$.

10°. *Если X — полностью определенный источник и условная энтропия введена указанным способом, то справедливо правило сложения энтропий $\mathcal{H}(X) + \mathcal{H}(Y|X) = \mathcal{H}(XY)$.*

Она согласована также с интерпретацией [2] условной энтропии как относительной сложности.

Если источник X, участвующий в произведении XY, недоопределен, применим к нему некоторое преобразование доопределения и при вычислении условной энтропии будем использовать полученное доопределение $\dot{X}$. Имеются содержательные основания для того, чтобы условную энтропию определить на базе лучшего доопределения $\hat{X}$ (считаем, что оно единственно). Переходные вероятности $p_{i|T}$ из утверждения 9°, задающие лучшее доопределение, позволяют найти совместные вероятности $p_{iU} = \sum_T p_{TU}p_{i|T}$ пар (a_i, b_U) в произведении $\hat{X}Y$, а по ним — условную энтропию $\mathcal{H}(Y|\hat{X})$, которая и используется в качестве $\mathcal{H}(Y|X)$.

В общем случае недоопределенных данных правило сложения энтропий заменяется некоторым обобщенным правилом. Его формулировка требует новых понятий. *Продолжением доопределения $\hat{X}$ на XY* называется полностью определенный источник $\hat{X}\dot{Y}$, построенный по $XY\hat{X}$ применением некоторого набора переходных вероятностей $p_{j|TUi} = p(b_j|a_T, b_U, a_i)$ и порождающий пары (a_i, b_j) с вероятностями $p_{ij} = \sum_{T,U} p_{TUi}p_{j|TUi}$. Величину $\hat{\mathcal{H}}(XY) = \min_{\hat{X}\dot{Y}} I(XY; \hat{X}\dot{Y})$, где I — взаимная информация и минимум берет-

ся по всем продолжениям $\hat{X}\dot{Y}$ лучшего доопределения $\hat{X}$, назовем *энтропией произведения XY при лучшем доопределении источника X*.

11°. *Имеет место обобщенное правило сложения энтропий*

$$\mathcal{H}(X) + \mathcal{H}(Y|X) = \hat{\mathcal{H}}(XY).$$

Следующее утверждение указывает необходимые и достаточные условия, при которых справедливо обычное правило сложения энтропий (не обобщенное).

12°. *Пусть $\hat{Q} = (\hat{q}_i,\, i \in M)$ и $Q^{(i)} = (q_j^{(i)},\, j \in L)$, $i \in M$, — наборы, на которых достигаются энтропии $\mathcal{H}(X)$ и $\mathcal{H}(Y|a_i)$. Чтобы для источников X и Y имело место правило сложения энтропий, необходимо и достаточно одновременное выполнение условий:*

(а) *на наборе $q_{ij} = \hat{q}_i q_j^{(i)}$, $i \in M$, $j \in L$, достигается энтропия $\mathcal{H}(XY)$,*

(б) *для любых $T \subseteq M$ и $U \subseteq L$ при каждом $i \in T$ сумма $\sum_{j \in U} q_j^{(i)}$ не зависит от i.*

Скажем, что источник X *конкретней* Y, если во всякой паре (a_T, b_U) такой, что $p_{TU} > 0$, выполнено $a_T \in A_0$ либо $b_U = *$. Утверждение 12° позволяет доказать следующий факт, обобщающий 10°.

13°. *Если источник X конкретней Y, то имеет место правило сложения энтропий.*

Работа выполнена при финансовой поддержке ОНИТ РАН по программе фундаментальных исследований.

Список литературы

1. Галлагер Р. Теория информации и надежная связь. — М.: Советское радио, 1974.

2. Колмогоров А. Н. Алгоритм, информация, сложность. — М.: Знание, 1991.

3. Нечипорук Э. И. О сложности вентильных схем, реализующих булевские матрицы с неопределенными элементами // ДАН СССР. — 1965. — Т. 163, № 1. — С. 40–42.

4. Шоломов Л. А. Сжатие частично определенной информации // Нелинейная динамика и управление. — Вып. 4. — М.: Физматлит, 2004. — С. 385–399.

5. Шоломов Л. А. Информационные свойства недоопределенных данных // Дискретная математика и ее приложения: Сборн. лекций молодежных научных школ. Вып. IV. — М.: ИПМ РАН, 2007. — С. 26–50.

6. Шоломов Л. А. О мере информации нечетких и частично определенных данных // ДАН. — 2006. — Т. 410. № 1. — С. 321–325.

7. Шоломов Л. А. Обобщенное правило сложения энтропий для недопределенных данных // ДАН. — 2009. — Т. 427, № 1. — С. 28–31.

ПРАВИЛЬНЫЕ МНОГОГРАННИКИ И МНОГОГРАННИКИ С ПРАВИЛЬНЫМИ ГРАНЯМИ ТРЕХМЕРНОГО ПРОСТРАНСТВА ЛОБАЧЕВСКОГО

В. С. Макаров (Москва)

Работа посвящена обзору некоторых новых результатов в теории правильных разбиений плоскости Лобачевского и выпуклых правильногранных многогранников трехмерного пространства Лобачевского. Такие многогранники с правильными гранями, как тела Платона (правильные многогранники) и тела Архимеда (равноугольно полуправильные многогранники), соответствующие им разбиения сферы на правильные сферические многоугольники, также как и паркетажи из равных правильных многоугольников плоскости Эвклида ("соты", квадрильяж, треугольный паркетаж) хорошо известны со времен древней Эллады.

Условимся относительно основных понятий и определений. Разбиение определяется как такое расположение тел в пространстве, которое является одновременно и покрытием и упаковкой. Известно, что если тела (клетки) разбиения — выпуклые, то они — многогранники. Разбиение пространства многогранниками называется нормальным, если многогранники смежны лишь по целым граням (далее мы будем рассматривать только такие). Согласно общепринятому, будем называть разбиение правильным, если группа симметрии этого разбиения действует транзитивно на множестве его клеток (тайлов). Разбиение пространства X^n постоянной кривизны (т. е. S^n, E^n, Λ^n) равными правильными многогранниками является примером правильного разбиения, но его группа симметрии значительно богаче, чем необходимо для обеспечения требования правильности: она действует транзитивно на множестве флагов этого разбиения. Напомним, что флаг — это совокупность вершины клетки, луча исходящего из этой вершины и идущего вдоль ребра клетки, и полуплоскости, содержащей двумерную грань, инцидентную, выделенному ребру. Условимся такие разбиения (на равные правильные

многогранники) называть платоновыми. Архимедовым разбиением условимся называть разбиение пространства на неравные правильные многогранники, обладающее группой симметрии, транзитивно действующей на множестве звезд его вершин. Звезда вершины (k-мерной клетки) — совокупность всех клеток, инцидентных рассматриваемой вершине (k-мерной клетке). Отметим, что разбиение, дуальное архимедову, является правильным; многогранные углы (гоноэдры) многогранника, дуального архимедову — правильные, что особенно ценно при построении разбиений пространства.

Все n-мерные платоновы и архимедовы тела и соответствующие разбиения n-мерного пространства постоянной кривизны были найдены во второй половине девятнадцатого века (Л. Шлефли [1], В. Шлегель [2], Т. Госсет [3]). Переводя на немецкий язык работы Лобачевского, Ф. Энгель заметил, что в пространстве Лобачевского естественно рассматривать и правильные бесконечные (с конечными гранями) многогранники, оси симметрии которых образуют параболическую или гиперболическую связку (проектирование этих многогранников лучами соответствующей связки на орисферу или на эквидистантную поверхность порождает платоновы разбиения на этих поверхностях). В. Ф. Каган [4] дал вывод таких правильных многогранников. Оказалось, что платоновых разбиений и, соответственно, правильных (платоновых) многогранников, вписанных в эквидистантные поверхности, ровно столько, сколько имеется решений в натуральных числах у неравенства $p^{-1} + q^{-1} < 2^{-1}$, $p \geq 3$, $q \geq 3$ (где p — число сторон 2-клетки, q — число 2-клеток, сошедшихся в вершине, см. [5, с. 95]). Соответствующий правильный многогранник (правильное разбиение) мы будем, следуя Л. Шлефли, обозначать символом $\{p, q\}$. Г. С. М. Коксетер к перечисленным правильным многогранникам предложил добавить предельные правильные многогранники (т. е. многогранники с бесконечно удаленными вершинами [6]).

Условимся и относительно обозначений трехмерных архимедовых многогранников (двумерных архимедовых разбиений) символом $(p_1, p_2, \ldots, p_k)$, указывающим, что в вершине многогранника (в узле разбиения) сходятся в указанной циклической последовательности правильные p_i-угольные грани (клетки). Для произвольного правильногранного (трехмерного) многогранника, на сколько известно, нет какого-нибудь удобного установившегося единообразного обозначения. Все выпуклые правильногранные многогранники трехмерного эвклидова пространства были найдены в середине 60-х годов прошлого века в работах В. А. Залгаллера [7] и Н. Джонсо-

на [8]. Их оказалось 92 (кроме призм и антипризм). Последнее время интерес к этой тематике резко возрос [9–11], рассматриваются обобщения обычных выпуклых правильногранных многогранников (в связи с некоторыми алгебраическими проблемами). Но вернёмся снова к правильным многогранникам. Если естественно рассматривать в трехмерном пространстве Лобачевского выше указанные правильные бесконечные многогранники, вписанные в орисферы или эквидистантные поверхности, то тогда нельзя отказывать в существовании и объектам на единицу меньшей размерности: правильным многоугольникам, вписанным в орициклы или эквидистанты [12]. Действительно, возьмем орицикл или эквидистанту, разобьем его (ее) на равные дуги, рассмотрим бесконечную ломаную, определяемую точками дробления, и выпуклый многоугольник, ею ограниченный. Очевидно, что этот многоугольник — выпуклый правильный многоугольник, вписанный в исходный орицикл (эквидистанту). Более того, если мы возьмем часть такого эквидистантного многоугольника, заключенную между его границей и базой эквидистанты, то, объединив эту часть с ее образом при отражении (или при подходящем скользящем отражении) в базе эквидистанты, мы получим новый правильный выпуклый многоугольник (вписанный в пару симметричных относительно общей базы эквидистант; "2-линза"). Полезно отметить, что аналогичный трехмерный объект (линзу, см., например, [13, с. 25]) тоже следовало бы считать правильным многогранником (В. Ф. Каган почему-то его не указал, возможно, из-за несвязности границы). Сразу отметим, что так полученные многоугольники, как легко видеть, разбивают плоскость Лобачевского и при этом в узле разбиения может сходиться любое наперед заданное число q многоугольников (для обозначения этих платоновых разбиений возможно подошел бы символ $\{\infty_{op}, q\}$ или символ $\{\infty_{экв}, q\}$).

Проделав с таким разбиением то, что мы обычно делаем с платоновыми разбиениями типа $\{p, q\}$ плоскости Лобачевского, когда хотим перейти от платонова разбиения $\{p, q\}$ к платонову трехмерному многограннику $\{p, q\}$ (через каждый узел разбиения проведем нормаль к базовой плоскости, отложим на каждой нормали по одну сторону от базовой плоскости по отрезку одной и той же длины и построим соответствующую многогранную поверхность), мы получим в трехмерном пространстве выпуклый правильный многогранник, гранями которого являются орициклические правильные многоугольники (в случае разбиения $\{\infty_{op}, q\}$ или эквидистантные правильные многоугольники в случае разбиения $\{\infty_{экв}, q\}$). При q,

равном 3, 4 или 5, вновь полученные правильные многогранники разбивают трехмерное пространство Лобачевского, что, в свою очередь, приводит к новым правильным многогранникам четырехмерного пространства Лобачевского и к новым правильным разбиениям этого пространства [12]. Но если мы хотим идти в направлении получения обобщенных правильных многогранников в пространствах Лобачевского высокой размерности, то для этого есть значительно более простой способ их получения (см., например, [13, с. 43–44]). Рассмотрим, например, правильный симплекс в Λ^3, вписанную в него сферу радиуса r и будем увеличивать радиус этой сферы. В некоторый момент $r = r_0$ вершины симплекса станут бесконечно удаленными точками (его двугранный угол при этом станет равным 60^o и потому на такие предельные правильные симплексы разбивается Λ^3). Увеличим еще немного радиус r до некоторого $r_1 > r_0$ так, чтобы вершины симплекса стали идеальными точками, а ребра превратились бы в прямые. Хорошо известно, что поляра такой идеальной вершины есть плоскость, ортогональная ко всем ребрам (и плоскостям граней), проходящим через эту идеальную вершину. Усекая такой запредельный симплекс полярами его идеальных вершин, мы получим усеченный симплекс. Плоскости его треугольных граней (назовем их черными) ортогональны соответствующим плоскостям шестиугольных граней (назовем их белыми). Если произвести отражения такого усеченного симплекса в плоскостях черных граней (и во всех их образах, получаемых при таких отражениях), то получим выпуклый правильный многогранник без вершин; все его ребра — прямые, а грани составлены из белых граней исходного симплекса (этот многогранник, так сказать, бесконечно "ветвится" в пространстве). Абсолютно очевидно, что аналогичные правильные выпуклые (разветвленные) многогранники можно получать в пространстве Лобачевского любой размерности из любого конечного (и не только) правильного многогранника: симплекса T^n, куба K^n или ортаэдра O^n. Мы здесь этим ограничимся, дабы не слишком усложнять ситуацию [13–15, 17] и для иллюстрации дальнейшего будем использовать лишь многогранники типов $\{\infty_{op}, q\}$ или $\{\infty_{экв}, q\}$) и не будем подыматься по размерности выше, чем $n = 4$. В настоящее время, мне кажется, наиболее интересным рассмотреть двумерные разбиения и соответствующие трехмерные многогранники.

Переходя от правильных (платоновых) многогранников к архимедовым (равноугольно полуправильным) всего естественнее было бы подробно проследить действие тех методов (приемов), которыми получаются конечные архимедовы многогранники и показать при-

менимость этих методов к рассмотренным выше простейшим бесконечным правильным выпуклым многогранникам (как с конечными, так и с бесконечными гранями) пространства Лобачевского. Интуитивно применимость соответствующих методов достаточно очевидна и потому мы ограничимся здесь лишь перечислением типов получаемых архимедовых многогранников пространства Лобачевского (архимедовых разбиений плоскости Лобачевского).

Из правильного многогранника $\{p, q\}$ (платонова разбиения $\{p, q\}$) методом усечения вершин получаются архимедовы многогранники $(2p, 2p, q)$, методом центрореберного усечения вершин получаются почти правильные многогранники (p, q, p, q), методом одновременного усечения и вершин и ребер (общий случай) — получаются архимедовы многогранники типа $(4, 2p, 2q)$, методом одновременного усечения и вершин и ребер (специальный случай) — получаются архимедовы многогранники типа $(p, 4, q, 4)$ и, наконец, методом "доворотов" граней — многогранники $(p, 3, q, 3, 3)$; в частном случае, многогранники — $(p, 3, p, 3, 3)$. Весьма любопытно отметить, что почти правильные многогранники (p, q, p, q) допускают обобщения $(p, q, p, q, \ldots, p, q)$, которые, в свою очередь, приводят к архимедовым многогранникам еще одной серии — $(q, 2p, k, 2p)$. Красивое обобщение допускают и многогранники вида $(p, 3, p, 3, 3)$ — они приводят к архимедовым многогранникам вида $(p, 3, p, 3, q, 3)$. Но все таки при таком подходе попытка получить все архимедовы многогранники пространства Лобачевского явно обречена на неудачу: достаточно вспомнить одну из старых конструкций (см., например, [17–18]), которую, применительно к нашему случаю можно сформулировать следующим образом:

Теорема 1 (о четносторонних архимедовых многогранниках). *Если в звезде сошлись только четноугольные правильные многоугольники с числами сторон* $2p_1$, $2p_2$, ..., $2p_k$, $k > 3$, *то архимедово разбиение плоскости Лобачевского с такой звездой* ($2p_1$, $2p_2$, ..., $2p_k$), *существует* (*при этом порядок следования четноугольников в звезде можно фиксировать произвольно*).

Правда, может быть было бы сперва более естественно доказать следующее простое утверждение:

Теорема 2 (существование звезды). *Если нам задан набор натуральных чисел* p_1, p_2, ... , p_k, *где* $k > 6$, *то на* Λ^2 *существует звезда, состоящая из* k *правильных* p_i*-угольников,* $i = 1,\ldots, k$, *в которой* p_i*-угольники сходятся в заданной нам последовательности* (*число* k *может быть уменьшено, если* p_i *достаточно велики; например, если все* $p_k \geq 7$, *то в качестве* k *достаточно взять*

число 3).

Доказательство. Обозначим через α_i^E — величину угла правильного p_i-угольника эвклидовой плоскости и через $\alpha_i^\Lambda(a)$ — величину угла правильного p_i-угольника плоскости Лобачевского (его величина зависит от длины $2a$ стороны этого многоугольника; читателю рекомендуется сделать чертеж или заглянуть в [18]). Очевидно, что величина $\alpha_i^\Lambda(a)$ непрерывно убывает от α_i^E до нуля при непрерывном возрастании a от нуля до $+\infty$. Так как $k > 6$ и $p_i \geq 3$, то сумма $\sum_{i=1}^k \alpha_i^E > 2\pi$ и, следовательно,

$$\lim_{a\to 0} \sum_{i=1}^{k} \alpha_i^\Lambda(a) > 2\pi.$$

В то же время

$$\lim_{a\to +\infty} \sum_{i=1}^{k} \alpha_i^\Lambda(a) = 0.$$

Следовательно, существует такое $a = a_0$, что $\sum_{i=1}^k \alpha_i^\Lambda(a_0) = 2\pi$. Поэтому, если при некоторой точке $O \in \Lambda^2$ (как при вершине) мы построим заданные нам p_i-угольники с так выбранной длиной $2a_0$ стороны, то мы и получим звезду ("протозвезду") из таких правильных многоугольников. При этом порядок следования многоугольников вокруг вершины может быть любым (и, следовательно, в частности многоугольники могут идти в заданном нам порядке p_1, p_2, ..., p_k). Справедливости ради, следует отметить, что утверждения теорем 1 и 2 были получены в разное время, разными авторами и независимо друг от друга. Далее, казалось бы, следовало бы постараться "разбавить" набор четноугольников за счет нечетноугольников (это удается сделать), но следующая теорема ставит преграду надежде получить все архимедовы разбиения, двигаясь в этом направлении.

Теорема 3. *Каков бы ни был заданный конечный набор правильных многоугольников, он всегда может быть пополнен единственным p-угольником, $p \leq 5$, так что из пополненного набора можно построить звезду, являющуюся звездой архимедова разбиения плоскости Лобачевского.*

Доказательство этой теоремы основано на использовании предложенной А. Пуанкаре классификации (по родам) планигонов плоскости Лобачевского. Отсюда естественно возникает идея классифицировать аналогичным образом (по родам) и все архимедовы разбиения плоскости Лобачевского, а вместе с тем и все архимедовы много-

гранники пространства Лобачевского с последующим более подробным изучением каждого класса, соответствующего данному роду. При этом в двумерном случае видимо можно, используя теорему о продолжении, достаточно эффективно привлекать различные алгоритмы для поиска соответствующих архимедовых многогранников при помощи вычислительной техники.

После сказанного о ситуации, сложившейся в проблеме классификации архимедовых многогранников, становится более или менее понятной и ситуация с описанием правильногранных многогранников трехмерного пространства Лобачевского Λ^3. Просматривая перечень правильных эквидистантных многогранников пространства Лобачевского, мы сразу видим, например, что звезда вершины разбиения $\{3, q\}$ есть правильная q-угольная пирамида ($q \geq 7$), что сразу дает счетную серию простых (в смысле [7]) правильногранных многогранников, существующих только в Λ^3. Взяв счетную серию архимедовых многогранников $(p, 4, 3, 4)$ и рассмотрев первую корону p-угольной грани, мы приходим к другой счетной серии правильногранных простых многогранников ("купола" — в терминологии [7]), присущей только лишь пространству Лобачевского (в пространстве Эвклида купола, как и пирамиды, существуют лишь при $p = 3, 4, 5$). Вычисленные в свое время двугранные углы предельных архимедовых многогранников [16], позволяют строить самые экзотические правильногранные ("разветвленные") многогранники в пространстве Лобачевского, а указанные выше методы получения архимедовых многогранников (пригодных к использованию для таких построений правильногранных многогранников), расширяют практически неограниченно класс правильногранных многогранников пространства Лобачевского [19]. Наконец, для размерностей $3, 4, 5$ следовало бы указать еще на совсем асимметричные правильногранные многогранники получаемые за счет использования кельвиновских упаковок (разбиений) [20].

Работа частично поддержана грантом РФФИ 08-01-00565.

Список литературы

1. Schlafli L. Reduction d'une Integrale Multiple qui comprend l'arc du cercle et l'aire du triangle spherique comme cas particuliers // Jornal de Mathematiques (1). — 1855. — V. 20. — P. 359–394.

2. Schlegel V. Theorie der homogen zusammengesetzten // Nova Acta Leop. Carol. — 1883. — Bd. 44. — P. 343–459.

3. Gosset T. On the regular and semi-regular figures in spaces of n dimensions // Messenger of Mathematics. — 1990. — V. 29. — P. 43–48.

4. Каган В. Ф. Основания геометрии. Ч. 1. — М.-Л., 1949; Ч. 2. — М.-Л., 1956.

5. Fejes Toth L. Regular figures. — Pergamon Press, 1964.

6. Coxeter H. S. M. Regular honeycombs in hyperbolic space // Proc. ICM 1954, v. 3. — Groningen-Amsterdam, 1956. — P. 155–169.

7. Залгаллер В. А. Выпуклые многогранники с правильными гранями // Труды ЛОМИ АН СССР. — 1967. — Т. 2.

8. Johnson N. W. Convex polyhedra with regular faces // Canad. J. Math. — 1966. — V. 18, № 1. — P. 169–200.

9. Макаров В. С., Макаров П. В. О выпуклых многогранниках с правильными гранями в пространстве Лобачевского // Материалы VIII Международного семинара "Дискретная математика и ее приложения". — М.: Изд-во мех-мат ф-та МГУ, 2004. — С. 402–405.

10. Залгаллер В. А., Гурин А. М. К истории изучения выпуклых многогранников с правильными гранями и гранями, составленными из правильных // Труды Математического Общества Санкт-Петербурга. — 2008. — Т. 14, № 4. — С. 215–294.

11. Тимофеенко А. В. Инволюции конечных групп и выпуклые правильногранники. — Автореферат диссертации на соискание ученой степени доктора физ.-матем. наук. — Екатеринбург, 2009.

12. Макаров В. С. О некоторых обобщенных правильных многогранниках пространства Лобачевского. // Материалы IX Международного семинара "Дискретная математика и ее приложения", посвященного 75-летию академика О. Б. Лупанова (18–23 июня 2007 г.). — М.: Изд-во механико-математического факультета МГУ, 2007. — С. 390–393.

13. Макаров В. С. Геометрические методы построения дискретных групп движений пространства Лобачевского // Проблемы геометрии. — 1983. — Т. 15. — С. 3–59.

14. Заморзаев А. М. О правильных многосторонниках и многогранниках в пространстве Лобачевского // Учен. Зап. Кишиневского гос. ун-та. — 1959. — Т. 39. — С. 195–207.

15. Заморзаев А. М., Русанов А. М. Правильные многогранники, описанные около сферы и орисферы в пространстве Лобачевского // Учен. Зап. Кишиневского гос. ун-та. — 1962. — Т. 50. — С. 45–54.

16. Макаров В. С., Пахомий А. П. О многогранника с правильными гранями в пространстве Лобачевского // VI Тираспольский симпозиум по общей топологии и ее приложениям. — Кишинев—Штиинца, 1991. — С. 159–160.

17. Макаров В. С. Полуправильные многоугольники и многосторонники на плоскостях Эвклида и Лобачевского // Учен. Зап. Кишиневского гос. ун-та. — 1960. — Т. 54. — С. 101–116.

18. Макаров В. С. Об одном классе двумерных федоровских групп // Изв. АН СССР. — 1967. Т. 31, № 3. — С. 531–542.

19. Макаров П. В. К вопросу о классификации разбиений плоскости Лобачевского — в печати.
20. Макаров П. В. О кельвиновских разбиениях трехмерного пространства Лобачевского правильными многогранниками // УМН. — 1990. — Т. 45, № 1 (271). — С. 179–180.

О ВЫДЕЛЕНИИ ЭФФЕКТИВНО РАЗРЕШИМЫХ ПОДКЛАССОВ В ЗАДАЧЕ ЦЕЛОЧИСЛЕННОГО ЛИНЕЙНОГО ПРОГРАММИРОВАНИЯ

А. Ю. Чирков (Нижний Новгород)

В первой части статьи дан краткий обзор результатов о числе вершин выпуклой оболочки целочисленных и частично целочисленных точек полиэдра. Приведены неулучшаемые (при фиксированной размерности) по порядку оценки числа вершин. Во второй части работы исследуется задача минимизации строго квазивыпуклой функции, заданной оракулом, на целочисленной решетке. В третьей части приведены результаты о задаче целочисленного линейного программирования с бимодулярной матрицей. Четвертая часть посвящена приближению оптимального решения задачи о рюкзаке оптимальными решениями задачи о рюкзаке с ограничениями на мощность решения.

1. Число вершин неявно заданного полиэдра

Пусть $P = \{x \in R^d : \ Ax \le b\}$, где $A \in Z^{m\times d}$, $b \in Z^m$. Выпуклая оболочка точек, принадлежащих $P \cap Z^d$, является полиэдром, который обозначим через P_I. Аналогично определяется частично целочисленный полиэдр P_k, как выпуклая оболочка точек $P \cap Z^k \times R^{d-k}$. Множество вершин полиэдра P обозначим через $V(P)$. Известно [1], что $|V(P)| \le \xi(d,m)$, где $\xi(d,m) = \binom{m-\lfloor\frac{d-1}{2}\rfloor-1}{\lfloor\frac{d}{2}\rfloor} + \binom{m-\lfloor\frac{d}{2}\rfloor-1}{\lfloor\frac{d-1}{2}\rfloor}$. В отличие от непрерывного случая, множество $V(P_I)$ может быть как угодно большим уже на плоскости [2]. Достижимые верхние оценки $|V(P_I)|$ в двумерном случае получены в работе [3].

Первые верхние оценки числа вершин P_I в d-мерном случае получены в [4]. Поскольку вершину полиэдра нельзя представить полусуммой других точек этого полиэдра, то из условий $x \in V(P_I)$ и

$y,\ 2x-y \in P_I$, следует, что $x = y$. На этом замечании основано понятие множества, обладающего свойством разделенности. Множество $M \subseteq \{x:\ x \in Z^d, x \geq 0\}$ обладает *свойством разделенности*, если из условий $z,\ y \in M$ и $2z \geq y$ следует, что $z = y$. Число элементов множества M, обладающего свойством разделенности, и лежащему в полосе $\{x:\ \psi_i \leq x_i \leq \omega_i,\ i = 1, 2, ..., d-1\}$ не превосходит $\prod_{i=1}^{d-1} \left(1 + \log_2 \frac{\omega_i+2}{\psi_i+1}\right)$.

Метод получения верхних оценок числа вершин состоит в отображении множества вершин P_I в ограниченное множество, обладающее свойством разделенности. Все существующие верхние оценки числа вершин P_I [5–12] получены именно таким методом. Различие в подходах связано только с разными способами построения отображений множества $V(P_I)$ в множество, обладающее свойством разделенности. Подход, дающий самые лучшие известные верхние оценки числа вершин полиэдра P_I изложен в [11]. Главная идея этого подхода заключается в разбиении полиэдра на (обобщенные) симплексы, с последующей оценкой числа вершин в каждом симплексе.

Для d-мерного полиэдра, заданного системой из m неравенств, существует разбиение на (обобщенные) симплексы, общим количеством не более $d!\xi(d, m+1)$ [14]. Оценив число вершин в каждом (обобщенном) симплексе из покрытия полиэдра P получим неравенство $|V(P_I)| \leq (d+1)!\xi(d, m+1)(1 + (d+2)^2 \log_2(d+1)\alpha)^{d-1}$. Для простого политопа P неравенство можно уточнить

$|V(P_I)| \leq (d+1)!|V(P)|(1 + (d+2)^2 \log_2(d+1)\alpha)^{d-1}$.

Число вершин частично целочисленного полиэдра оценивается как

$|V(P_k)| \leq \binom{d}{k} (k+1)!\xi(d, m+1)(1 + (d+2)^2 \log_2(d+1)\alpha)^{k-1}$.

Если политоп задан системой неравенств с вещественными коэффициентами, а δ — его диаметр, то

$|V(P_I)| \leq (d+1)!\xi(d, m+2d+1)(1 + (d+1)^3 \log_2(d+1)\delta)^{d-1}$,

$|V(P_k)| \leq (k+1)!\xi(k, 3k+2) \binom{d}{k} \xi(d, m)(1+(k+1)^3 \log_2(k+1)\delta)^{k-1}$.

Если политоп P_I телесный (имеет ненулевой объем), то

$|V(P_I)| \leq (d+1)!\xi(d, m+2d+1)(1 + (d+1)^3 \log_2(d!Vol(P)))^{d-1}$.

Подход, позволяющий показать невозможность улучшения полученных ранее верхних оценок сформулирован в работах [15, 16]. Центральная идея этого подхода заключается в следующем. Для простого политопа $P = \{x:\ Ax \leq b\}$, где $A \in Z^{m \times d}$, $b \in Z^m$, $rgA = d \leq m$ рассматривается множество политопов $P(c, \beta)$, полученных из P аф-

финным преобразованием $x = \frac{1}{2d\delta\Delta^2}(E_c y + \beta e_1)$. Здесь E_c — матрица, отличающаяся от единичной матрицы первой строкой, равной c ($c_1 \neq 0$), Δ — максимум из абсолютных значений миноров порядка d матрицы A. На множестве политопов $P(c, \beta)$, где $\beta \in [0, \delta - 1]$, $c_1 = \delta$ и $c_i \in [0, \delta - 1]$ при $i \geq 2$, определим среднее число вершин $\sigma(P, \delta)$.

Пусть $\omega_d(t) = \sum_{i=1}^{d} \frac{(-1)^{i+1} t^{d-i}}{(d-i)!}$. Для среднего числа вершин доказано неравенство $\sigma(P, \delta) \geq 0,25 d^{-d} |V(P)| \omega_d(\ln(\delta) - d \ln(1 + d + d\Delta))$. Подход переносится и на частично целочисленные политопы.

В [17] конструктивно доказано существование d-мерного полиэдра P, заданного системой из $2d^2$ неравенств с рациональными коэффициентами, что $|V(P_I)| = O(l^{d-1})$, где l — длина двоичной записи коэффициентов системы. Однако для построения полиэдров с большим числом вершин требуется значительный объем вычислений.

2. Минимизация строго квазивыпуклой функции на целочисленной решетке

На задачу минимизации строго квазивыпуклой функции на целочисленной решетке можно смотреть как на обобщение задачи целочисленного линейного программирования. Будем считать, что функция $f(x)$ задана оракулом, позволяющим сравнить значения функции в точках целочисленной решетки.

Множество точек $M \subset Z^d$ назовем *разрешающим* для $f(x)$, если для любого $x \in Z^d$ найдутся такие точки $x_1, ..., x_k \in M$, что $f(x_1) \leq ... \leq f(x_k)$ и $x_k \in conv(x_1, ..., x_{k-1}, x)$. Поскольку значение $f(x)$ в любой внутренней точке политопа меньше, чем в его вершинах, то включение $x_k \in conv(x_1, ..., x_{k-1}, x)$ возможно только при выполнении неравенства $f(x_k) < f(x)$.

Разрешающее множество M содержит точку минимума и является "доказательством" минимальности этой точки. Любая строго квазивыпуклая функция g, удовлетворяющая тем же соотношениям на точках M, что и f имеет ту же самую точку минимума. Разрешающее множество назовем *минимальным*, если удаление любой его точки приводит к множеству, не являющимся разрешающим.

Теорема. *На целочисленной решетке Z^d для произвольной строго квазивыпуклой функции существует минимальное разрешающее множество, число элементов которого ограничено константой γ_d, зависящей только от d.*

Имеется верхняя оценка на эту константу — $\gamma_d \leq 2^{d^3}$.

В качестве примера рассмотрим задачу минимизации строго квазивыпуклой функции на отрезке $[a,b]_I$. Минимальное разрешающее множество состоит из трех подряд идущих точек (или дух соседних точек на концах отрезка). Количество различных минимальных разрешающих множеств равно $b-a+1$. Обращение к оракулу в любой паре точек позволяет разделить множество разрешающих множеств на две части. Таким образом, любой алгоритм затратит в худшем случае не менее $\log_2(b-a+1)$ обращений к оракулу. Метод деления отрезка пополам имеет такую же оценку трудоемкости в худшем случае.

Знание структуры минимальных разрешающих множеств позволяет получать нижнюю оценку трудоемкости всех алгоритмов минимизации строго квазивыпуклой функции. В [18] получено описание минимальных разрешающих множеств для двумерной целочисленной решетки.

Пусть точки $x_1, x_2, x_3, x_4 \in Z^2$ удовлетворяют условиям:

1) $\det(x_2 - x_1, x_3 - x_1) = -\det(x_2 - x_1, x_4 - x_1) = 1$;

2) выполнены неравенства $f(x_1) \le f(x_2) \le f(x_3)$, $f(x_2) \le f(x_4)$, $f(x_1) \le f(2x_1 - x_2)$, $f(x_3) \le f(x_3 \pm (x_1 - x_2))$, $f(x_4) \le f(x_4 \pm (x_1 - x_2))$.

Тогда множество из 9 точек $T = \{x_1, x_2, x_3, x_4, 2x_1 - x_2, x_3 \pm (x_1 - x_2), x_4 \pm (x_1 - x_2)\}$ является разрешающим множеством для строго квазивыпуклой функции $f(x)$.

К сожалению, в случае большей размерности описание минимальных разрешающих множеств пока не получено. Пусть $m_d(r)$ — количество минимальных разрешающих множеств, содержащихся в кубе $\{x : |x|_\infty \le r\}$. Справедливо неравенство $m_d(r) \ge m_{d-1}(r)^3$. Поскольку $m_1(r) = 2r-1$, то $m_d(r) \ge (2r-1)^{3^{d-1}}$. Следовательно, трудоемкость в худшем случае произвольного алгоритма минимизации не меньше $\log_2 m_d(r) \ge 3^{d-1}\log_2(2r-1)$.

Если строго квазивыпуклая функция задана оракулом, позволяющим вычислить ее значение в любой точке целочисленной решетке, то трудоемкость любого алгоритма минимизации не меньше $\log_2 m_d(r) \ge \frac{3^{d-1}\log_2(2r-1)}{2d+\log_2\log_2 2r}$.

3. Задача целочисленного линейного программирования с бимодулярной матрицей

Матрицу назовем *бимодулярной*, если все ее миноры максимального порядка равны $0, \pm 1, \pm 2$. Пусть $P = \{x : Ax \le b\}$, A бимоду-

лярна, $b \in Z^m$. Данная задача рассматривалась в работах [19 , 20]. Имеет место

Теорема. *Если P телесно, то P_I не пусто.*

Из теоремы вытекает эффективный алгоритм проверки совместности системы линейных неравенств с бимодулярной матрицей. Имеется интересная связь между полиэдрами P и P_I.

Теорема. *Вершины P_I лежат на ребрах P.*

Для вершины v определим конус $K(v)$, образованный неравенствами, обращающимися в равенство в точке v. Справедливы включения

- $V(K(v)_I) \subseteq V(P_I)$,
- $\cup_{v \in V(P)} V(K(v)_I) = V(P_I)$.

4. О приближении решения задачи о рюкзаке

Пусть $L(a,b) = \{x : \ x \in Z^d, ax \leq b, \ x \geq 0\}$, $G(a,b) = \{x : \ x \in Z^d, \ ax \geq b, \ x \geq 0\}$. Множество, полученное из множества M удалением точек с $d-k$ не нулевыми компонентами, обозначим через M_k. Рассмотрим следующие задачи:

- $\max_{x \in L(a,b)} cx$ — задача о рюкзаке;
- $\max_{x \in L_k(a,b)} cx$ — задача о рюкзаке с ограничением на мощность решения;
- $\min_{x \in L(a,b)} cx$ — минимизационная задача о рюкзаке;
- $\min_{x \in L_k(a,b)} cx$ — минимизационная задача о рюкзаке с ограничением на мощность решения.

Оптимальные решения этих задач обозначим через x^*, y^*, x', y', соответственно. Введем величины: $\alpha_{k\,d} = \inf_{a,b,c} \frac{cx'}{cx^*}$ — гарантированная точность задачи о рюкзаке, $\beta_{k\,d} = \inf_{a,b,c} \frac{cy^*}{cy'}$ — гарантированная точность минимизационной задачи о рюкзаке

Справедливы [21] равенства $\alpha_{d-1\,d} = \frac{2^d-2}{2^d-1}$ и $\beta_{d-1\,d} = 1 - 2^{1-d}$. Первое равенство достигается, например в следующей задаче

$\max \sum_{i=1}^{d} 2^{i-1} x_i$;
$\sum_{i=1}^{d} (2^{d+i-1} + 2^{d-i}) x_i \leq 4^d - 1$.

Второе равенство достигается как точная нижняя грань. Пусть числа $\mu, \nu \in Z_+$ удовлетворяют неравенствам $\nu > \mu > 2^d$. Для задачи

$\max\left(2^{d-1}x_1+\mu\sum_{i=2}^{d}2^{i-2}x_i\right)$,

$x_1+\nu\sum_{i=2}^{d}3^{i-2}x_i\le 1+\nu(3^{d-1}-1)/2$.

справедливо равенство $\frac{cy*}{cy'}=\mu^{-1}+1-2^{1-d}$, и, следовательно, $\beta_{d-1\,d}=1-2^{1-d}$.

Из полученных равенств несложно вывести оценки $\frac{2^{k+1}-2}{2^{k+1}-1}\ge\alpha_{k\,d}\ge\frac{2^d-2^{d-k}}{2^d-1}$ и $1-2^{-k}\ge\beta_{k\,d}\ge(1-2^{1-d})...(1-2^{-k})$.

Для случая $k=1$ известны точные значения α_{1d} и $\beta_{1d}=1/2$.

Определим последовательности чисел $\delta_1=1$, $\delta_k=\delta_{k-1}(\delta_{k-1}+1)$, при $k\ge 2$, и $\sigma_1=1$, $\sigma_k=1+\sigma_{k-1}(\delta_{k-1}+1)$, при $k\ge 2$. Справедливо равенство $\alpha_{1d}=\delta_d/\sigma_d$. Величина α_{1d} вычислена в [22].

Список литературы

1. Бренстед А. Введение в теорию выпуклых многогранников. — М.: Мир, 1988.

2. Rubin D. S. On the unlimited number of faces in integer hulls of linear programs with a single constraint // Operations Research. — 1970. — V. 18, № 5. — P. 940–945.

3. Веселов С. И., Шевченко В. Н. О числе экстремальных точек квадратной системы линейных неравенств. — Деп. в ВИНИТИ, № 450-79-деп.

4. Шевченко В. Н. О числе крайних точек в целочисленном программировании // Кибернетика. — 1981. — № 2. — С. 133–134.

5. Hayes A. S., Larman D. C. The vertices of the knapsack polytope // Discrete Applied Mathematics. — 1983. — № 6. — P.135–138.

6. Шевченко В. Н. Алгебраический подход в целочисленном программировании // Кибернетика. — 1984. — № 4. — С. 36–41.

7. Morgan D. A. Upper and lower bound results on the convex hull of integer points in polyhedra // Mathematika. — 1991. — V. 38. — P. 321–328.

8. Чирков А. Ю. О числе крайних точек в задаче целочисленного линейного программирования // Комбинаторно-алгебраические методы в дискретной оптимизации: Межвуз. сб. — Н. Новгород, 1991. — С. 157–159.

9. Шевченко В. Н. Верхние оценки числа крайних точек в целочисленном программировании // Математические вопросы кибернетики. Вып. 4. — М., 1992. — С. 65–72.

10. Cook W., Hartman A., Kannan R., McDiarmid C. On integer points in polihedra // Combinatorica. — 1992. — V. 12. № 1. — P. 27–37.

11. Чирков А. Ю., Шевченко В. Н. О числе вершин выпуклой оболочки пересечения полиэдра с целочисленной решеткой // Ниже-

гор. ун-т. им. Н. И. Лобачевского, Нижний Новгород,1993. — Деп.в ВИНИТИ 29.07.93, № 2165–В93.

12. Шевченко В. Н. Качественные вопросы целочисленного программирования. — М.: Физматлит, 1995.

13. Чирков А. Ю, Веселов С. И. О вершинах неявно заданных целых полиэдров // Вестник Нижегородского университета им. Н. И. Лобачевского. — 2008. — № 1. — 118–123.

14. Чирков А. Ю. Теорема Каратеодори и покрытие многогранника симплексами // Нижегор. ун-т им. Н. И. Лобачевского, Нижний Новгород, 1993. — Деп. в ВИНИТИ 19.03.93, № 668–В93.

15. Веселов С. И. Нижняя оценка среднего числа неприводимых и крайних точек в двух задачах дискретного программирования // Горьк. ун-т, Горький, 1984. — Деп. в ВИНИТИ 3.06.84, № 619–В84.

16. Чирков А. Ю. О нижней оценке числа вершин выпуклой оболочки целочисленных и частично целочисленных точек полиэдра // Дискретный анализ и исследование операций. — 1996. — Т. 3, № 2. — С. 80–89.

17. Barany I., Howe R., Lovasz L. On integer points in polyhedra: a lower bound // Combinatorica. — 1992. — V. 12 (2). — P. 135–142.

18. Чирков А. Ю. Минимизация квазивыпуклой функции на двумерной целочисленной решетке // Вестник Нижегородского университета им. Н. И. Лобачевского. — Сер. Математическое моделирование и оптимальное управление. — 2003. — Вып. 1 (26). — С. 227–237.

19. Веселов С. И., Чирков А. Ю. О задаче целочисленного программирования с бимодулярной матрицей // Комбинаторно-алгебраические и вероятностные методы и их применение. — Горький: Изд-во ГГУ, 1990. — С. 107–110.

20. Veselov S. I., Chirkov A. Yu. Integer program with bimodular matrix // Discrete Optimization. — 2009. — V. 6 (2). — P. 220–222.

21. Чирков А. Ю., Шевченко В. Н. О приближении оптимального решения целочисленной задачи о ранце оптимальными решениями целочисленной задачи о ранце с ограничением на мощность // Дискретный анализ и исследование операций. Сер. 2. — 2006. — Т. 13, № 2. — С. 56–73.

22. Kohli R., Krishnamurti R. Joint performance of greedy heuristics for the integer knapsack problem // Discrete Appled Mathematics. — 1995. — V. 56. — P. 37–48.

О ЗАДАЧАХ Д. КНУТА И Р. БЕЛЛМАНА, ИХ ОБОБЩЕНИЯХ И БЛИЗКИХ ВОПРОСАХ

В. В. Кочергин (Москва)

1. Постановка задач. Некоторые известные результаты

В докладе рассматриваются различные задачи, тесно связанные с известной проблемой наискорейшего возведения в степень, исследуются общие закономерности и различия этих задач, а также дается обзор последних результатов автора в данном направлении.

Классический вопрос о наиболее экономичном по числу используемых операций умножения способе возведения в степень обычно формулируется на аддитивном языке как задача об аддитивных цепочках [1] для натурального числа и допускает следующее обобщение.

Пусть $A = (a_{ij})$ — целочисленная матрица размера $p \times q$ с неотрицательными элементами без нулевых строк. *Векторной аддитивной цепочкой для матрицы* A называется последовательность q-мерных векторов (наборов) вида $\mathbf{v}_1 = e_1, \mathbf{v}_2 = e_2, \ldots, \mathbf{v}_q = e_q, \mathbf{v}_{q+1}, \mathbf{v}_{q+2}, \ldots, \mathbf{v}_{q+r}$, начинающаяся с q единичных векторов и удовлетворяющая условиям: 1) для каждого k, $k \geq q+1$, найдутся такие i и j, $i \leq j < k$, что $\mathbf{v}_k = \mathbf{v}_i + \mathbf{v}_j$ (сложение векторов покомпонентное); 2) $\{(a_{11}, a_{12}, \ldots a_{1q}), \ldots, (a_{p1}, a_{p2}, \ldots a_{pq})\} \subseteq \{\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_{q+r}\}$. Число r называется длиной цепочки. Минимальная длина аддитивной цепочки для матрицы A называется *аддитивной сложностью матрицы* A и обозначается через $l(A)$.

Задача об аддитивной сложности матриц по-существу совпадает с известной задачей о сложности вычисления систем одночленов [2, 3] (систем коммутативных мономов) — величина $l(A)$ численно равна минимально возможному числу операций умножения, достаточному для вычисления по переменным $x_1, x_2, \ldots, x_q$ задаваемой матрицей A системы одночленов $x_1^{a_{11}} x_2^{a_{12}} \ldots x_q^{a_{1q}}, \ldots, x_1^{a_{p1}} x_2^{a_{p2}} \ldots x_q^{a_{pq}}$ (при этом допускается многократное использование промежуточных результатов). Для величины $l(A)$ используется также обозначение $l(x_1^{a_{11}} x_2^{a_{12}} \ldots x_q^{a_{1q}}, \ldots, x_1^{a_{p1}} x_2^{a_{p2}} \ldots x_q^{a_{pq}})$.

Помимо описанной вычислительной модели, которую условно можно назвать *«Вычисление системы одночленов»* («Входы»: $x_1, x_2, \ldots, x_q$; используемые операции: умножение; вычисляемые функции: $x_1^{a_{11}} x_2^{a_{12}} \ldots x_q^{a_{1q}}$, $\ldots$, $x_1^{a_{p1}} x_2^{a_{p2}} \ldots x_q^{a_{pq}}$; мера сложности: $l(A)$) будем рассматривать еще две близкие модели [4–6] — *«Вычисление системы целочисленных линейных форм»* («Входы»: $x_1, x_2, \ldots, x_q$; используемые операции: сложение и вычитание; вычисляемые функции: $a_{11}x_1 + \ldots + a_{1q}x_q$, $\ldots$, $a_{p1}x_1 + \ldots + a_{pq}x_q$, мера

сложности: $l_2(A)$) и *«Вычисление системы элементов свободной абелевой группы»* («Входы»: $x_1, x_2, \ldots, x_q, x_1^{-1}, x_2^{-1}, \ldots, x_q^{-1}$; используемые операции: умножение; вычисляемые функции: $x_1^{a_{11}} x_2^{a_{12}} \ldots x_q^{a_{1q}}$, $\ldots$, $x_1^{a_{p1}} x_2^{a_{p2}} \ldots x_q^{a_{pq}}$; мера сложности: $l_F(A)$).

Отметим, что для всех этих трех моделей при представлении процесса вычисления в виде ориентированного графа (по-существу, в виде схемы из функциональных элементов) сложностью является число невходовых вершин, причем полустепень захода любой невходовой вершины равна 2. Если же перейти к мере сложности, связанной с числом ребер, и отказаться от ограничений на полустепень захода, то придем к следующей вычислительной модели [7, 8] — *«Реализация целочисленных матриц вентильными схемами с кратными путями»*.

Итак, пусть $A = (a_{ij})$ — целочисленная матрица размера $p \times q$ с неотрицательными элементами. Ориентированный граф S без ориентированных циклов будем называть *вентильной схемой с кратными путями* (или *вентильной схемой с предписанным числом путей*), *реализующей матрицу* A, если:

1) в S выделено p вершин — входных полюсов и q вершин — выходных полюсов, причем в S нет ориентированных путей от одного входа к другому, от одного выхода к другому, от выхода к входу;

2) для любой пары (i, j), $1 \le i \le p$, $1 \le j \le q$, число ориентированных путей от i-го входа к j-му выходу равно в точности a_{ij}.

Сложность $l_{BC}(S)$ вентильной схемы S — это число ребер (вентилей) в схеме S. Положим $l_{BC}(A) = \min l_{BC}(S)$, где минимум берется по всем схемам, реализующим матрицу A.

Среди значительного количества публикаций по данной теме (см., например, обзоры [9, 10]) выделим наиболее важные.

А. Брауэр в 1939 г. доказал, что $l(n) \sim \log n$, установив верхнюю оценку $l(n) \le \log n + \frac{\log n}{\log\log n} + O\left(\frac{\log n \log\log\log n}{(\log\log n)^2}\right)$. Здесь и далее считаем логарифм двоичным, если явно не указано основание.

В 1960 г. П. Эрдёш установил асимптотическую неулучшаемость этой оценки для почти всех n: при любом $\varepsilon > 0$ для почти всех n

$$l(n) \ge \log n + (1 - \varepsilon)\frac{\log n}{\log\log n}.$$

При этом стоит отметить разную природу слагаемых в правой части этого соотношения — слагаемое $\log n$ связано с величиной числа n и должно присутствовать для любого значения n, а «энтропийное» слагаемое (отношение логарифма количества чисел, не превосходящих n, к повторному логарифму) зависит от «строения» числа n и присутствует для «почти всех» n, причем несмотря на то, что

для почти всех n второе слагаемое присутствует, для индивидуальных последовательностей существенных продвижений в доказательстве нижних оценок по сравнению с результатом 1975 г. А. Шенхаге ($l(n) \geq \log n + \log s(n) - 2{,}13$, где $s(n)$ — число единиц в двоичной записи числа n, и, следовательно, $\log s(n) \leq \log\log n$) получено не было.

В 1963 г. Р. Беллман поставил задачу о сложности вычисления одночлена $x_1^{a_1} \dots x_q^{a_q}$, т. е. о нахождении величины $l((a_1, \dots, a_q))$.

В 1969 г. Д. Кнут поставил задачу о сложности вычисления набора степней $x^{a_1} \dots x^{a_p}$, т. е. о нахождении величины $l((a_1, \dots, a_p)^T)$.

При фиксированных q и p для задач Беллмана и Кнута получены асимптотически точные решения в 1964 г. Е. Страусом и в 1975 г. А. Яо соответственно. В обоих случаях сложность асимптотически совпадает с величиной $\log(\max a_i)$.

В 1981 г. независимо А. Ф. Сидоренко; Дж. Оливос; Д. Кнут и К. Пападимитриу установили, что задачи Беллмана и Кнута эквивалентны (и, следовательно, следует говорить о «задаче Беллмана — Кнута»). Более точно — для любой целочисленной матрицы A с неотрицательными элементами размера $p \times q$ без нулевых строк и столбцов выполняется равенство

$$l(A) + p = l\left(A^T\right) + q.$$

Для меры сложности l_2 для любой целочисленной матрицы A размера $p \times q$ выполняются неравенства $-q \leq l_2\left(A^T\right) - l_2(A) \leq p$.

В отличие от мер сложности l и l_2, мера сложности l_F не обладает свойством двойственности:

$$l_F\left(\left(2^k, -2^k\right)\right) = k + 1, \quad l_F\left(\left(2^k, -2^k\right)^T\right) = 2k.$$

Для меры сложности l_{BC} равенство $l_{BC}(A) = l_{BC}(A^T)$ очевидно.

В 1981 г. П. Доуни, Б. Леонг и Р. Сети показали, что задача распознавания по набору натуральных чисел $(n_1, n_2, \dots, n_p, l)$ существования аддитивной цепочки, имеющей длину l и содержащей числа $n_1, n_2, \dots, n_p$, является NP-полной. Поэтому естественно рассматривать исходные задачи в асимптотической постановке (при $\sum |a_{ij}| \to \infty$) — требуется найти метод вычисления матрицы A со сложностью в том или ином смысле близкой к значению $l(A)$, $l_2(A)$, $l_F(A)$ или $l_{BC}(A)$ соответственно (для всех или почти для всех матриц).

2. Задача Беллмана — Кнута

Теорема 1 [11, 12]. Положим $N = n_1 n_2 \dots n_m$. Тогда при $N \to \infty$

$$l(n_1, n_2, \dots, n_m) \lesssim \log(\max n_i) + \frac{\log N}{\log\log N} + m,$$

Доказательство этой теоремы существенно опирается на результаты О. Б. Лупанова, Э. И. Нечипорука, Н. Пиппенджера и автора по теории классических вентильных схем.

Верхняя оценка теоремы 1 асимптотически неулучшаема для почти всех наборов, причем даже в более сильной второй вычислительной модели:

Теорема 2 [13]. *Для любого $\varepsilon > 0$ и произвольной последовательности наборов $\tilde{n}(s) = \big(n_1(s), n_2(s), \dots, n_{m(s)}(s)\big)$, удовлетворяющей при $s \to \infty$ условию $m(s) = o\left(\log\left(\max_i n_i(s)\right) + \frac{\log N(s)}{\log\log N(s)}\right)$, где $N(s) = \prod_{i=1}^{m(s)} n_i(s)$, доля наборов из множества*

$$\{(k_1, k_2, \dots, k_m) \mid k_i \in \mathbb{N},\ 1 \le k_i \le n_i,\ i = 1, 2, \dots, m\},$$

для которых выполняется неравенство

$$l_2\left((k_1, k_2, \dots, k_m)\right) \ge \log\left(\max_i n_i\right) + (1 - \varepsilon)\frac{\log N}{\log\log N},$$

стремится к 1 при $s \to \infty$.

Таким образом, с учетом верхней оценки в условиях теоремы 2 для почти всех наборов справедливо соотношение

$$l\left((k_1, k_2, \dots, k_m)\right) \sim \log\left(\max_i k_i\right) + \frac{\log K}{\log\log K}, \quad \text{где } K = k_1 k_2 \dots k_m.$$

3. Одно применение задачи Кнута

Рассмотрим задачу о сложности порождения двоичных слов схемами конкатенации. Пусть $\tilde{\alpha}$ — двоичный набор, $l_c(\tilde{\alpha})$ — минимальное число операций конкатенации, достаточное для получения из символов 0 и 1 набора $\tilde{\alpha}$. Положим: A_n^k — множество всех двоичных наборов длины n, содержащих ровно k единиц, $l_c(k, n) = \max_{\tilde{\alpha} \in A_n^k} l_c(\tilde{\alpha})$, $k = 0, 1, \dots, n$. Доопределим выражение $\log C_n^k / \log\log C_n^k$ при $k = 0$ и $k = n$ нулем. С использованием теорем 1 и 2 устанавливается

Теорема 3 [14]. *Пусть $0 \le k_m \le n_m$, $m = 1, 2, \dots$; $n_m \to \infty$ при $m \to \infty$. Тогда*

$$l_c(k_m, n_m) \sim \log n_m + \frac{\log C_{n_m}^{k_m}}{\log\log C_{n_m}^{k_m}}.$$

4. Функции Шеннона

При $K \geq 2$ положим $L(p,q,K) = \max l(A)$, $L_2(p,q,K) = \max l_2(A)$, $L_F(p,q,K) = \max l_F(A)$, $L_{BC}(p,q,K) = \max l_{BC}(A)$ (в первом и четвертом равенствах максимум берется по всем матрицам размера $p \times q$, удовлетворяющим условиям $a_{ij} < K$, а во втором и третьем — по всем матрицам размера $p \times q$, удовлетворяющим условиям $|a_{ij}| < K$).

Теорема 4 [3, 7, 15, 16]. *При условии* $pq \log K \to \infty$

$$L(p,q,K) = \min(p,\, q) \log K + \frac{pq \log K}{\log(pq \log K)}(1 + o(1)) + O(p+q),$$

$$L_2(p,q,K) = \min(p,\, q) \log K + \frac{pq \log(2K-1)}{\log(pq \log K)}(1 + o(1)) + O(p+q),$$

$$L(p,q,K) = \min(p,\, q+1) \log K + \frac{pq \log(2K-1)}{\log(pq \log K)}(1 + o(1)) + O(p+q),$$

$$L_{BC}(p,q,K) = 3 \min(p,\, q) \log_3 K + \frac{pq \log K}{\log(pq \log K)}(1 + o(1)) + O(p+q).$$

Первое и последнее соотношение установлены Н. Пиппенджером.

Особо отметим возможность асимптотически оптимальных вычислений во второй модели с использованием помимо сложений ровно одной операции вычитания.

5. Универсальная нижняя оценка

Пусть $D(A)$ — это максимум абсолютных величин миноров матрицы A, где максимум берется по всем минорам.

Теорема 5 [6, 8]. *Для любой ненулевой целочисленной матрицы* A *справедливы неравенства:*

$$l(A) \geq \log D(A), \quad l_2(A) \geq \log D(A),$$
$$l_F(A) \geq \log D(A), \quad l_{BC}(A) \geq 3 \log_3 D(A)$$

(*в первом и последнем неравенствах подразумевается, что в матрице* A *нет нулевых строк и все ее элементы неотрицательны*).

Оценки сложности через величину определителя были известны ранее; впервые такие соображения использовались, по-видимому, Ж. Моргенстерном (1973). Универсальность теоремы 5 заключается в том, что она справедлива для всех четырех мер сложности

и для произвольной (вычислимой в данной модели) матрицы. При этом оценка теоремы 5 дает хорошую отправную точку для получения асимптотически точных оценок для индивидуальных последовательностей матриц (естественно, изучаются те соотношения параметров, когда первые слагаемые в равенствах из теоремы 4 дают определяющий вклад, в частности, когда параметры p и q ограничены или фиксированы).

6. Сложность вычисления целочисленных линейных форм

Для этой задачи получено асимптотически окончательное решение — при фиксированных (и даже слабо растущих) p и q удалось доказать верхнюю оценку, асимптотически совпадающую с оценкой, устанавливаемой теоремой 5:

Теорема 6 [4]. *Пусть последовательность целочисленных матриц $A(n)$ размера $p(n) \times q(n)$ при $n \to \infty$ удовлетворяет условию $p(n) + q(n) = o((\log\log D(A(n)))^{1/2})$. Тогда*

$$l_2(A(n)) \sim \log D(A(n)).$$

Результат предыдущей теоремы переносится на следующую (промежуточную) вычислительную модель. Через $l_{\{-\}}(A)$ обозначим минимально возможное число операций вычитания, достаточное для вычисления по переменным $x_1, x_2, \ldots, x_q$, системы линейных форм $\{a_{i1}x_1 + a_{i2}x_2 + \ldots + a_{iq}x_q, \quad i = 1, 2, \ldots, p\}$, задаваемых целочисленной матрицей коэффициентов A.

Обозначим через φ «золотое сечение», т. е. величину $\frac{\sqrt{5}+1}{2}$. Тогда в условиях теоремы 6 справедливо соотношение [17]:

$$l_{\{-\}}(A) \sim \log_\varphi D(A(n)).$$

7. Сложность вычисления систем одночленов

Для матриц «малой» размерности для данной модели вычислений, объединяя результаты нескольких работ (см, например, [2, 6]), также удается установить верхнюю оценку вида $\log D(A) + o(\log D(A))$:

Теорема 7 [2, 6]. *Для произвольной последовательности целочисленных матриц $A(n)$ размеров $p \times 2$, $2 \times q$ или 3×3 (p и q — ограничены)*

$$l\,(A(n)) \sim \log D(A(n).$$

Уже в простейшем случае, когда матрицы имеют размер 2×2, при всей прозрачности основной идеи доказательства верхней оценки, само доказательство технически является довольно громоздким, не дающим особой надежды распространить его на матрицы больших размеров. Для упрощения дальнейших доказательств вводится вспомогательная существенно усиленная вычислительная модель, разрешающая дополнительно к операции сложения использовать умножение на произвольное неотрицательное рациональное число, не превосходящее 2. Для этой модели, с одной стороны, доказывать верхние оценки существенно проще (например, задача о сложности вычислении натурального числа в этой модели становится тривиальной — очевидно, что для получения числа n требуется $\lceil \log n \rceil$ операций), и которая, с другой стороны, допускает при некоторых естественных условиях переход к вычислению в исследуемых моделях без асимптотического увеличения сложности. Однако доказательство верхней оценки для матриц размера 3×3 даже в существенно усиленной модели технически сложно [2]. Частично природу возникающих при доказательстве трудностей объясняет «предельность» случая матриц размера 3×3 — уже для матриц размера 4×4 аналогичная асимптотика, вообще говоря, может и не иметь места.

Пусть $A(t, n)$ — квадратная матрица порядка $2t$ $(t \geq 2)$; первой строкой матрицы $A(t, n)$ является набор длины $2t$, первая половина разрядов которого равна n, а вторая половина — 0. Остальные $2t-1$ строк матрицы $A(t, n)$ получаются из первой строки последовательным циклическим сдвигом на один разряд вправо.

Теорема 8 [18]. *Пусть* $t \leq \log n / \log\log n$. *Тогда*

$$l(A(t, n)) \sim \frac{2t}{t+1} \log D(A(t, n)).$$

Таким образом, приведен пример последовательности матриц размера $2t \times 2t$, для которой устанавливаемую теоремой 5 нижнюю оценку в рамках первой вычислительной модели можно усилить асимптотически в $2t/(t+1)$ раз.

Следствием этой теоремы является тот факт, что при вычислении системы одночленов, задаваемой матрицей $A(t, n)$, при $t \geq 3$ при всех достаточно больших n в силу неравенств $\frac{2t}{t+1} \log x \geq 1,5 \log x > \log_{\varphi} x$ более эффективной операцией является не умножение, а деление.

8. Реализация матриц вентильными схемами с кратными путями

Для этой вычислительной модели с помощью модификации методов из работ [2, 6], устанавливаются аналогичные результаты.

Теорема 9 [8]. *Для произвольного натурального m и произвольной последовательности матриц $\{A_n\}$ с неотрицательными элементами, каждая из которых имеет размер либо $2 \times q_n$, где $q_n \leq m$, либо $p_n \times 2$, где $p_n \leq m$, либо 3×3, при условии $D(A_n) \to \infty$ выполняется соотношение*

$$l_{BC}(A_n) \sim 3 \log_3 D(A_n).$$

Теорема 10 [8]. *При условии $t = o\left(\frac{\log n}{\log \log n}\right)$ справедливо асимптотическое равенство*

$$l_{BC}(A(t,n)) \sim \frac{6t}{t+1} \log_3 D(A(t,n)).$$

Таким образом и для этой вычислительной модели нижняя оценка из теоремы 5 асимптотически неулучшаема для матриц размера $p \times 2$, $2 \times q$ и 3×3, а для матриц большего размера, вообще говоря, может быть улучшена.

9. Сложность вычисления систем элементов свободных абелевых групп

Для третьей вычислительной модели даже для матриц «малой» размерности оценка из теоремы 5 может быть усилена. Положим $T(A) = \max\limits_{i,k;j}\{-a_{ij}a_{kj}\}$.

Теорема 11 [5]. *Пусть последовательность целочисленных матриц $A(n) = (a_{ij}(n))$ размера $2 \times q(n)$ удовлетворяет условию $q(n) = o(\log \log \max\limits_{i,\,j} |a_{ij}(n)|)$. Тогда*

$$l_F(A(n)) \sim \log \max\{D(A(n)), T(A(n))\}.$$

Теорема 12 [5]. *Для произвольной последовательности целочисленных матриц $A(n)$ размера 3×2*

$$l_F(A(n)) \sim \log \max\{D(A(n)), T(A(n)), R(A(n))\}.$$

Отметим, что величина $R(A)$ определяется довольно нетривиально, но конструктивно [5], и в последнем соотношении эта величина может быть определяющей — например, для матрицы A, соответствующей системе элементов $\{x^{-n}, x^n, y^n\}$, выполняются равенства $D(A) = T(A) = n^2$, $R(A) = n^3$.

В заключение отметим, что использование не очень сильной, на первый взгляд, возможности использовать помимо единичных векторов противоположных к ним векторов, может существенно снизить сложность:

Теорема 13 [18]. *При условии* $t = o(\log n)$

$$\frac{l(A(t,n))}{l_F(A(t,n))} \sim \frac{2t}{t+1}.$$

Работа выполнена при финансовой поддержке РФФИ (проект 08–01–00863) и программы поддержки ведущих научных школ РФ (проект НШ–4437.2010.1).

Список литературы

1. Кнут Д. Е. Искусство программирования для ЭВМ. Т. 2. — М.: Мир, 1977.

2. Кочергин В. В. О сложности вычисления системы из трех одночленов от трех переменных // Математические вопросы кибернетики, вып . 15. — М.: Физматлит, 2006. — С. 79–155.

3. Pippenger N. On evaluation of powers and monomials // SIAM J. Comput. — 1980. — V. 9, N 2. — P. 230–250.

4. Кочергин В. В. Об асимптотике сложности аддитивных вычислений систем целочисленных линейных форм // Дискретный анализ и исследование операций. Серия 1. — 2006. — Т. 13, № 2. — С. 38–58.

5. Кочергин В. В. О сложности совместного вычисления трех элементов свободной абелевой группы с двумя образующими // *Дискретный анализ и исследование операций. Серия* 1. — 2008. — Т. 15, № 2. — С. 23–64.

6. Кочергин В. В. О сложности вычисления систем одночленов и систем целочисленных линейных форм // Дискретная математика и ее приложения. Сборник лекций молодежных научных школ по дискретной математике и ее приложениям. Выпуск III. — М.: Изд-во механико-математического факультета МГУ, 2007. — С. 3–63.

7. Pippenger N. The mimimum number of edges in graphs with prescribed paths // Math. Systems Theory. — 1979. — V. 12, № 4. — P. 325–346.

8. Кочергин В. В. О сложности вентильных схем с кратным числом путей // Материалы XVIII Международной школы-семинара «Синтез и сложность управляющих систем» имени академика О. Б. Лупанова (Пенза, 28 сентября – 03 октября 2009 г.). — М.: Изд-во механико-математического факультета МГУ, 2009. — С. 51–56.

9. Gordon D. M. A survey of fast exponentiation methods // Journal of Algorithms. — 1998. — V. 27. — P. 129–146.

10. Subbarao M. V. Addition chains — some results and problems // Number Theory and Applications. Editor R. A. Mollin. NATO Advanced Science Institutes Series: Series C. — Kluwer Academic Publisher Group, 1989. — V. 265. — P. 555–574.

11. Гашков С. Б., Кочергин В. В. Об аддитивных цепочках векторов, вентильных схемах и сложности вычисления степеней // Методы дискретного анализа в теории графов и сложности. — Новосибирск, 1992. — Вып. 52. — С. 22–40.

12. Кочергин В. В. О сложности аддитивных вычислений // Современные проблемы математики и механики. Том III. Математика. Выпуск 3. Дискретная математика. — М.: Изд-во Московского университета, 2009. С. 51–75.

13. Кочергин В. В. О сложности вычислений одночленов и наборов степеней // Дискретный анализ. — Новосибирск: Издательство Института математики СО РАН, 1994. — (Тр./РАН. Сиб. отделение. Ин-т математики; Т. 27) — С. 94–107.

14. Кочергин В. В. О мультипликативной сложности двоичных слов с заданным числом единиц // Математические вопросы кибернетики, вып. 8. — М.: Наука, 1999. — С. 63–76.

15. Кочергин В. В. Об аддитивных вычислениях систем целочисленных линейных форм // Вестник Московского университета. Сер. 1. Математика. Механика. — 1993. — № 6. — С. 97–101.

16. Кочергин В. В. О максимальной сложности совместного вычисления систем элементов свободной абелевой группы // Вестник Московского университета. Сер. 1. Математика. Механика. — 2007, № 3. — С. 14–19.

17. Кочергин В. В. О сложности аддитивных вычислений, использующих только операции вычитания // Труды VIII Международной конференции «Дискретные модели в теории управляющих систем» (Москва, 6–9 апреля 2009 г.). — М.: Издательский отдел факультета ВМиК МГУ имени М. В. Ломоносова; МАКС Пресс, 2009. — С. 174–179.

18. Кочергин В. В. Об одном соотношении двух мер сложности вычисления систем одночленов // Вестник Московского университета. Сер. 1. Математика. Механика. — 2009. — № 4. — С. 8–13.

Секция «Синтез, сложность и надежность управляющих систем»

О НАДЕЖНОСТИ СХЕМ ПРИ ОДНОТИПНЫХ КОНСТАНТНЫХ НЕИСПРАВНОСТЯХ НА ВЫХОДАХ ЭЛЕМЕНТОВ

М. А. Алехина (Пенза)

Рассматривается реализация булевых функций схемами из ненадежных функциональных элементов в произвольном полном конечном базисе B. Будем считать, что схема из ненадежных функциональных элементов реализует функцию $f(x_1, ..., x_n)$, если при поступлении на входы схемы набора $\tilde{a} = (a_1, ..., a_n)$ при отсутствии неисправностей на выходе схемы появляется значение $f(\tilde{a})$. Все элементы схемы независимо друг от друга с вероятностью γ $(0 < \gamma < 1/2)$ переходят в неисправные состояния типа 0 на выходах элементов. Эти неисправности характеризуются тем, что в исправном состоянии функциональный элемент реализует приписанную ему булеву функцию φ, а в неисправном – константу 0. Неисправности типа 1 на выходах элементов определяются аналогично.

Далее считаем, что базисные элементы подвержены неисправностям типа 0 на выходах.

Пусть $P_{\bar{f}(\tilde{a})}(S, \tilde{a})$ — вероятность появления значения $\bar{f}(\tilde{a})$ на выходе схемы S, реализующей функцию $f(\tilde{x})$ при входном наборе $\tilde{a}$. Ненадежность $P(S)$ схемы S равна $\max\{P_{\bar{f}(\tilde{a})}(S, \tilde{a})\}$, где максимум берется по всем наборам $\tilde{a}$. Надежность схемы S равна $1 - P(S)$.

Пусть $P_\gamma(f) = \inf P(S)$, где S — схема, реализующая $f(\tilde{x})$. Схему A, реализующую f, назовем асимптотически оптимальной по надежности, если $P(A) \sim P_\gamma(f)$ при $\gamma \to 0$.

Нетрудно проверить, что ненадежность любой схемы, реализующей неконстантную функцию и содержащую хотя бы один функциональный элемент, не меньше γ.

Очевидно, функции x_i можно реализовать абсолютно надежно (не используя функциональных элементов), а функции, для реализации которых достаточно i элементов ($i \in \{1, 2, 3\}$) с ненадежностью $i\gamma$. Для любой функции в произвольном полном базисе справедлива теорема 1.

Теорема 1. *При* $\gamma \in (0, 1/960]$ *любую булеву функцию* f *можно реализовать такой схемой* A, *что* $P(A) \leq 3\gamma + 100\gamma^2$.

Известно [1], что в произвольном полном конечном базисе пяти элементов достаточно, чтобы реализовать хотя бы одну любую из функций $g(x_1, x_2, x_3, x_4) = x_1^{c_1}\&x_2^{c_2} \vee x_1^{c_1}\&x_3^{c_3} \vee x_2^{c_2}\&x_3^{c_3}$ или $g(x_1, x_2, x_3, x_4) = x_1^{c_1}\&x_2^{c_2} \vee x_3^{c_3}\&x_4^{c_4}$ или $g(x_1, x_2, x_3, x_4) = (x_1^{c_1} \vee x_2^{c_2})\&(x_3^{c_3} \vee x_4^{c_4})$, $c_i \in \{0, 1\}, i = 1, 2, 3, 4$. Обозначим множество этих функций через G.

Лемма 1 [2]. *Допустим, что произвольную функцию* f *можно реализовать схемой* S *с ненадежностью не больше* p. *Пусть* S_g — *схема, реализующая некоторую функцию множества* G *с ненадежностью не больше* p, *причем* v_0 — *вероятность ошибки схемы* G *на наборе* (c_1, c_2, c_3, c_4) *соответственно, а* v_1 — *на наборе* $(\bar{c}_1, \bar{c}_2, \bar{c}_3, \bar{c}_4)$ *соответственно. Тогда схема* $\Phi(S)$ *реализует функцию* f *с ненадежностью* $P(\Phi(S)) \leq \max\{v_0, v_1\} + 10p^2$.

Лемма 2 [3]. *При* $\gamma \in (0, 1/960]$ *любую булеву функцию* f *можно реализовать такой схемой* S, *что* $P(S) \leq 24\gamma$.

Теперь можем пояснить идею доказательства теоремы 1. Пусть B — произвольный полный конечный базис. Построим в нем схему S_g, состоящую из не более пяти элементов и реализующую некоторую функцию множества G и вычислим вероятности v_0 на наборе (c_1, c_2, c_3, c_4) и v_1 на наборе $(\bar{c}_1, \bar{c}_2, \bar{c}_3, \bar{c}_4)$ соответственно. Во всех случаях оказалось, что $\max\{v_0, v_1\} \leq 3\gamma$.

Обозначим f^c функцию $\bar{f}$ при $c = 0$ и функцию f при $c = 1$.

Возьмем схемы $S^{c_1}, S^{c_2}, S^{c_3}, S^{c_4}$, реализующие функции $f^{c_1}, f^{c_2}, f^{c_3}, f^{c_4}$ соответственно с ненадежностью не более 24γ (по лемме 2 это возможно), а также схему S_g и построим схему $\Phi(S)$. Используя лемму 1, оценим ненадежность схемы $\Phi(S)$ и получим $P(\Phi(S)) \leq 3\gamma + 5760\gamma^2 \leq 9\gamma$. Проделаем еще три шага итерации и построим схемы $\Phi^2(S)$, $\Phi^3(S)$, $\Phi^4(S)$, для ненадежностей которых по лемме 1 выполняются неравенства:

$P(\Phi^2(S)) \leq 3\gamma + 810\gamma^2 \leq 3,85\gamma$;

$P(\Phi^3(S)) \leq 3\gamma + 147,8\gamma^2 \leq 3,154\gamma$;

$P(\Phi^4(S)) \leq 3\gamma + 99,5\gamma^2$.

Схема $\Phi^4(S)$ — искомая.

Из теоремы 1 следует, что при неисправностях типа 0 на выходах элементов при $\gamma \in (0, 1/960]$ надежные схемы A для всех булевых функций $f(x_1, ..., x_n)$, функционируют с ненадежностью $P(A) \leq 3\gamma + 100\gamma^2$.

Известно [2], что в общем случае константу 3 в оценке ненадежности понизить нельзя. Например, для почти всех функций в базисе $\{x_1 \& x_2, \bar{x_1}\}$ асимптотически оптимальные схемы функционируют с ненадежностью, асимптотически равной 3γ при $\gamma \to 0$.

Поскольку ненадежности двойственных схем равны [4], теорема 1 верна в произвольном полном конечном базисе при неисправностях типа 1 на выходах базисных элементов.

Список литературы

1. Аксенов С. И. О надежности схем над произвольной полной системой функций при инверсных неисправностях на выходах элементов // Известия высших учебных заведений. Поволжский регион. Естественные науки. — 2005. — № 6 (21). — С. 42–55.

2. Алехина М. А. Синтез асимптотически оптимальных по надежности схем. — Пенза: ИИЦ ПГУ, 2006.

3. Алехина М. А., Васин А. В. О надежности схем в базисах, содержащих функции не более чем трех переменных // Ученые записки Казанского государственного университета. Сер. Физико-математические науки — 2009. — Т. 151, кн 1. — С. 10–19.

4. Алехина М. А., Пичугина П. Г. О надежности двойственных схем в полном конечном базисе // Материалы XVIII Международной школы-семинара "Синтез и сложность управляющих систем" (Пенза 28 сентября – 3 октября 2009 г.). — М.: Изд-во мех.-мат. ф-та МГУ, 2009. — С. 10–13.

О СЛОЖНОСТИ ВОЗВЕДЕНИЯ В СТЕПЕНЬ ПРИ ОГРАНИЧЕНИЯХ НА ИСПОЛЬЗУЕМУЮ ПАМЯТЬ

К. С. Балакин (Москва)

Рассматривается классическая задача о сложности возведения в степень — нахождении минимального числа операций умножения, достаточного для возведения некоторого числа x в заданную степень n. Обычно эту задачу формулируют на языке аддитивных цепочек [1]: найти минимальную длину $l(n)$ аддитивной цепочки для числа n. Очевидно, что $l(n) \geq \log n$ (здесь и далее под обозначением $\log n$ понимается $\log_2 n$). А. Брауэр установил [2] асимптотику роста величины $l(n)$, доказав, что $l(n) \leq \log n + O(\frac{\log n}{\log \log n})$. Но приведенный в доказательстве алгоритм требует растущего с ростом n числа ячеек памяти. Возникает естественный вопрос об исследовании сложности в случае фиксированного числа ячеек памяти.

Обозначим через $l_t(n_1, \ldots, n_k)$, где $t \geq k$, минимальную длину аддитивной цепочки, вычисляющей набор чисел $n_1, \ldots, n_k$ с использованием не более t ячеек памяти. Считаем, что ячейки таковы, что в них можно записать любое требуемое число, но только одно.

Утверждение 1. *Для любого фиксированного t, $t \geq 2$, при условии $n \to \infty$ справедливо соотношение $l_t(n) \asymp \log n$.*

Этот простой факт следует из очевидной нижней оценки $\log n \leq l_t(n)$ и неравенств $l_t(n) \leq l_2(n) \leq \log n + v(n)$, где $v(n)$ — число единиц в двоичной записи числа n. Последнее неравенство вытекает из бинарных методов возведения в степень (как "справа налево" [2, с. 483–484], так и "слева направо" [2, с. 482–483]), требующих лишь 2 ячейки памяти.

Отметим, что оценка $l_2(n) \leq \log n + v(n)$ при $n = 2^k - 1$ (т. е. в "худшем случае") превращается в неравенство $l_2(n) \leq 2 \log n$. Покажем, что в этом случае при использовании двух ячеек памяти можно возвести в степень n со сложностью $\log n(1 + o(1))$.

Лемма. *Для любых натуральных u, v справедливо соотношение $l_2(u, v) \leq 2(\log u + \log v)$.*

Доказательство будем вести индукцией по $u+v$. База индукции очевидна. Далее, если среди чисел u и v хотя бы одно — четное (скажем, u), то, с использованием предположения индукции, имеем: $l_2(u, v) \leq l_2(u/2, v) + 1 \leq 2(\log(u/2) + \log v) + 1 < 2(\log u + \log v)$.

Если же и u, и v — нечетные (считаем, что $u > v$), то, учитывая предположение индукции, получаем: $l_2(u, v) \leq l_2((u - v)/2, v) + 2 \leq 2(\log((u - v)/2) + \log v) \leq 2(\log u + \log v)$.

Утверждение 2. *Для чисел вида $n = 2^k - 1$ справедлива оценка $l_2(n) \sim \log n$ при $n \to \infty$.*

Доказательство. Положим $s = \lceil \sqrt{k} \rceil, q = \lceil \frac{k}{s} \rceil, s' = k - s\lfloor \frac{k}{s} \rfloor$.

Тогда $n = a_0 + 2^s(a_1 + 2^s(\ldots + 2^s a_{q-1})\ldots)$, где $a_0 = \ldots = a_{q-2} = 2^s - 1, a_{q-1} = 2^{s'} - 1$. Следовательно, применяя лемму, имеем:

$$l_2(n) \leq sq + q + l_2(2^s - 1, 2^{s'} - 1) \leq \log n + O(\sqrt{\log n}).$$

Может возникнуть предположение, что для любого числа n величина $l_2(n)$ асимптотически не превосходит $\log n$. Оказывается, это не так.

Теорема. *Для любого фиксированного t, $t \geq 2$, найдется такое $\varepsilon = \varepsilon(t) > 0$, что при $n \to \infty$ доля чисел k из множества $\{1, \ldots, n\}$, удовлетворяющих условию $l_t(k) \geq (1+\varepsilon) \log n$, стремится к 1.*

Доказательство будем вести на языке аддитивных цепочек. Под *удвоением* будем понимать лишь удвоение максимального из хранящихся в памяти чисел, удвоения меньших членов будем относить к *неудвоениям*.

Оценим сверху число цепочек длины не более $(1+\varepsilon)\log n$, вычисляющих k, где $\frac{n}{\log n} < k \le n$.

Пусть длина цепочки равна r, $r \le (1+\varepsilon)\log n$, число удвоений равно $(1-\delta)\log n$. Тогда, учитывая [1, с. 490–491], что $n \le 2^{d-1}F_{p+3}$, где d — число удвоений, p — неудвоений, F_i — i-й член последовательности Фибоначчи, получаем (здесь $\gamma = (\sqrt{5}+1)/2$): $\frac{n}{\log n} < k < 2^{(1-\delta)\log n}F_{(\varepsilon+\delta)\log n+3} \sim n^{1-\delta}\gamma^{(\varepsilon+\delta)\log n+3} = n\gamma^3\left(\frac{\gamma^{\varepsilon+\delta}}{2^\delta}\right)^{\log n}$.

Поэтому $\gamma^{\varepsilon+\delta} \ge 2^\delta$ и, следовательно, $\delta \le \frac{\varepsilon\log\gamma}{1-\log\gamma} < 3,22\varepsilon$.

Теперь оценим величину N_t — число возрастающих аддитивных цепочек, соответствующих вычислениям с двумя ячейками памяти, длины не более $(1+\varepsilon)\log n$ с числом удвоений не менее чем $(1-\delta)\log n$:

$$N_t \le C^{(\varepsilon+\delta)\log n}_{(1+\varepsilon)\log n} \cdot \left(t\left(t-1+\tfrac{t(t-1)}{2}\right)\right)^{(\varepsilon+\delta)\log n} \cdot \prod_i (s_i+1)^{t-1}.$$

Первый сомножитель отвечает за количество вариантов выбора мест для неудвоений, второй — за выбор конкретных неудвоений (удвоить в любой из ячеек число, кроме максимального, либо перемножить содержимое любых двух ячеек, и по t вариантов, в какую ячейку сохранить результат), третий — за выбор тех значений, что сохраняются в остальных ячейках после участка из s_i удвоений.

Покажем, что, соответствующим образом выбрав ε, можно добиться того, что N_t будет не превосходить величины n^α, где $\alpha < 1$. Отдельно оценим каждый из сомножителей.

При условии

$$(1+\varepsilon)\log(1+\varepsilon) - 4,22\varepsilon\log 4,22\varepsilon - (1-3,22\varepsilon)\log(1-3,22\varepsilon) < \frac{1}{4} \quad (1)$$

выполняются неравенства

$$C^{(\varepsilon+\delta)\log n}_{(1+\varepsilon)\log n} < C^{4,22\varepsilon\log n}_{(1+\varepsilon)\log n} \lesssim \left(\frac{(1+\varepsilon)^{1+\varepsilon}}{(4,22\varepsilon)^{4,22\varepsilon}(1-3,22\varepsilon)^{1-3,22\varepsilon}}\right)^{\log n} < n^{\frac{1}{4}}.$$

Далее, при условии

$$4,22\varepsilon < \frac{1}{3(\log(t(t^2+t-2))-1)} \quad (2)$$

справедливо неравенство

$$\left(t\left(t-1+\frac{t(t-1)}{2}\right)\right)^{(\varepsilon+\delta)\log n} < n^{\frac{1}{3}}.$$

И, наконец, при условии

$$4,22\varepsilon \log \frac{4}{\varepsilon} < \frac{1}{3(t-1)} \tag{3}$$

выполняются соотношения

$$\prod_i (s_i+1)^{t-1} \le \left(\frac{2(1+\varepsilon)\log n}{(\varepsilon+\delta)\log n}\right)^{(t-1)(\varepsilon+\delta)\log n} \le$$

$$\left(\left(\frac{4}{\varepsilon+\delta}\right)^{(t-1)(\varepsilon+\delta)}\right)^{\log n} < \left(\frac{4}{\varepsilon}\right)^{4,22\varepsilon(t-1)\log n} < n^{\frac{1}{3}}.$$

В неравенствах (1)–(3) левые части неравенств стремятся к 0 при $\varepsilon \to 0$, и, следовательно, соотношения (1)–(3) будут справедливы при достаточно малом ε и фиксированном t. Доказательство завершено.

Таким образом, с фиксированным числом ячеек памяти добиться даже асимптотически оптимальных вычислений в задаче возведения в степень невозможно.

Работа выполнена при финансовой поддержке РФФИ (проект 08–01–00863), программы поддержки ведущих научных школ РФ (проект НШ–4437.2010.1) и программы фундаментальных исследований ОМН РАН «Алгебраические и комбинаторные методы математической кибернетики и информационные системы нового поколения».

Список литературы

1. Кнут Д. Е. Искусство программирования для ЭВМ. Т. 2. — М.: Мир, 1977.

2. Brauer A. On addition chains // Bull. Amer. Math. Soc. — 1939. — V. 45. — P. 736–739.

ЛЕГКОТЕСТИРУЕМЫЕ СХЕМЫ ДЛЯ ДИЗЪЮНКЦИИ

С. Р. Беджанова (Москва)

Будем рассматривать схемы из функциональных элементов в произвольном полном конечном базисе [1, 2], реализующие дизъюнкцию n переменных, где $n \ge 3$. В схемах допускается инверсная неисправность выхода ровно одного из элементов, то есть, если в исправном состоянии элемент реализует функцию φ, то при его поломке на выходе элемента реализуется функция $\overline{\varphi}$.

Пусть S — произвольная схема, реализующая функцию $f(\tilde{x}) = x_1 \vee \cdots \vee x_n$. Функция, реализуемая на выходе схемы при наличии в схеме неисправного элемента, называется функцией неисправности. Пусть g_1, ..., g_k — все возможные попарно различные нетривиальные функции неисправности; функция неисправности называется нетривиальной, если она отлична от исходной функции, реализуемой исправной схемой. Множество T булевых наборов длины n называется единичным диагностическим тестом, если для любой пары функций из $\{g_1, \ldots, g_k, f\}$ в T найдется набор, на котором значения этих функций различны. Длиной теста называется число наборов в нем. Среди всех схем, реализующих $f(\tilde{x})=x_1 \vee \cdots \vee x_n$, будем выделять те, которые допускают тесты минимальной возможной длины. В данной работе при исследовании единичных тестов рассматриваются неизбыточные схемы [3](при наличии в схеме неисправного элемента на выходе неизбыточной схемы реализуется нетривиальная функция неисправности).

Теорема. *Функция $f(\tilde{x})=x_1 \vee \cdots \vee x_n$ может быть реализована неизбыточной схемой, допускающей единичный диагностический тест не более чем из двух наборов.*

Доказательство теоремы конструктивное. В нем используется предложенное в [4] разбиение всех полных базисов на следующие (возможно, пересекающиеся) классы: 1) $\{x \vee y, \overline{x}\}$; 2) $\{x \vee \overline{y}, \overline{x}\}$; 3) $\{xy, \overline{x}\}$; 4) $\{\overline{xy}\}$; 5) $\{\overline{x \vee y}\}$; 6) $\{x\overline{y}, \overline{x}\}$; 7) базисы, содержащие функцию $x \vee y$; 8) базисы, содержащие функцию xy; 9) базисы, содержащие функцию $x \vee \overline{y}$; 10) базисы, содержащие функцию $x\overline{y}$; 11) базисы, содержащие функцию $xy \oplus xz \oplus yz \oplus \alpha_1 x \oplus \alpha_2 y \oplus \alpha_3 z \oplus \alpha_4$.

При переходе в неисправное состояние выходного элемента схемы в произвольном базисе, реализующей в исправном состоянии функцию $f(\tilde{x})$, на выходе схемы получается функция неисправности $g(\tilde{x}) = \overline{f}(\tilde{x})$. Для каждого из рассматриваемых базисов строятся схемы, удовлетворяющие следующему условию: на выходе неисправной схемы помимо функции $g(\tilde{x})$ могут быть реализованы только лишь булевы константы. Для того, чтобы различить функции неисправности $g(\tilde{x}) = \overline{f}(\tilde{x})$, $h(\tilde{x}) \equiv 0$, $d(\tilde{x}) \equiv 1$ между собой и отличить их от $f(\tilde{x})$, в тест достаточно включить два набора, например, $\tilde{0}$ и $\tilde{1}$.

Установлено, что оценка, приведенная в утверждении теоремы, в общем случае неулучшаема. В частности показано, что не существует схемы в базисе $\{x \vee y, \overline{x}\}$, реализующей дизъюнкцию $x_1 \vee \cdots \vee x_n$ и допускающей единичный диагностический тест из одного набора.

Работа выполнена при финансовой поддержке РФФИ (проект 08–01–00863), программы поддержки ведущих научных школ РФ

(проект НШ–4437.2010.1) и программы фундаментальных исследований ОМН РАН «Алгебраические и комбинаторные методы математической кибернетики и информационные системы нового поколения».

Список литературы

1. Лупанов О. Б. Асимптотические оценки сложности управляющих систем. — М.: Изд-во МГУ, 1984.

2. Редькин Н. П. Дискретная математика. — М.: Изд-во ЦПИ при механико-математическом факультете МГУ. 2007.

3. Редькин Н. П. Надежность и диагностика схем. — М.: Изд-во МГУ. 1992.

4. Редькин Н. П. Единичные проверяющие тесты для схем при инверсных неисправностях элементов // Математические вопросы кибернетики. Вып. 12. — 2003. — С. 217–230.

СИНТЕЗ ЛЕГКОТЕСТИРУЕМЫХ СХЕМ ДЛЯ СИСТЕМ БУЛЕВЫХ ФУНКЦИЙ

Ю. В. Бородина (Москва)

Пусть S — некоторая схема из функциональных элементов, реализующая систему (упорядоченный набор) из m булевых функций $f_1(\tilde{x}), f_2(\tilde{x}), \ldots, f_m(\tilde{x})$, $\tilde{x} = (x_1, x_2, \ldots, x_n)$.

Функции, реализуемые на выходах схемы при наличии в схеме неисправных элементов, называются *функциями неисправности*. Набор функций неисправности $(g_1(\tilde{x}), \ldots, g_m(\tilde{x}))$ будем называть нетривиальным, если хотя бы одна какая-нибудь функция $g_i(\tilde{x})$, $i \in \{1, \ldots, m\}$, отлична от соответствующей ей функции $f_i(\tilde{x})$, т.е. $g_i(\tilde{x}) \not\equiv f_i(\tilde{x})$.

Множество T входных наборов схемы S называется *полным проверяющим тестом* для этой схемы, если для любого нетривиального набора функций неисправности $(g_1(\tilde{x}), \ldots, g_m(\tilde{x}))$ в T найдется хотя бы один такой набор $\tilde{\sigma}$, что $(f_1(\tilde{\sigma}), \ldots, f_m(\tilde{\sigma})) \neq (g_1(\tilde{\sigma}), \ldots, g_m(\tilde{\sigma}))$ (здесь равенство булевых наборов, как обычно, покомпонентное, т.е. $(\alpha_1, \ldots, \alpha_m) = (\beta_1, \ldots, \beta_m)$ означает $\alpha_1 = \beta_1, \ldots, \alpha_m = \beta_m$). Число наборов, составляющих этот тест, называется длиной теста [1].

В качестве тривиального теста всегда можно взять тест, содержащий все 2^n наборов значений переменных булевой функции от n переменных.

В докладе рассматривается задача построения легкотестируемых схем из функциональных элементов в базисе $\{\&, \vee, {}^-\}$ для систем булевых функций в случае константных неисправностей типа "1" на выходах элементов.

Пусть $\mathcal{F}_{n,m}$ — система из m булевых функций $f_1(\tilde{x}), \ldots, f_m(\tilde{x})$, где $\tilde{x} = (x_1, x_2, \ldots, x_n)$; у функций из $\mathcal{F}_{n,m}$ могут быть фиктивные переменные из числа $x_1, x_2, \ldots, x_n$.

Согласно теореме 2 из работы [2], каждую из функций $f_1, \ldots, f_m$ можно реализовать схемой, допускающей полный проверяющий тест длины не более 2. Таким образом, систему $\mathcal{F}_{n,m}$ можно реализовать схемой, допускающей полный проверяющий тест длины не более $2m$. Эту очевидную оценку можно уменьшить, используя детали доказательства указанной теоремы.

Теорема 1. *Любую систему $\mathcal{F}_{n,m}$ из m булевых функций, отличных от констант, можно реализовать схемой из функциональных элементов, допускающей полный проверяющий тест длины не более $q+1$, где $q \leq m$ — число функций из $\mathcal{F}_{n,m}$, сохраняющих единицу (т. е. равных 1 на наборе $(1, \ldots, 1)$).*

Значение $q+1$ в этой оценке длины теста в общем случае нельзя заменить ни на какое число, меньшее q. Однако для систем монотонных функций это значение можно уменьшить.

Теорема 2. *Любую систему $\mathcal{F}_{n,m}$ из m монотонных булевых функций, отличных от констант, можно реализовать схемой из функциональных элементов, допускающей полный проверяющий тест длины 1.*

Работа выполнена при финансовой поддержке РФФИ (проект 08–01–00863), программы поддержки ведущих научных школ РФ (проект НШ–4437.2010.1) и программы фундаментальных исследований ОМН РАН «Алгебраические и комбинаторные методы математической кибернетики и информационные системы нового поколения».

Список литературы

1. Редькин Н. П. О схемах, допускающих короткие тесты // Вестник Московского университета. Серия 1. Математика. Механика. — 1988. — № 2.— С. 17–21.

2. Бородина Ю. В. Синтез легкотестируемых схем в базисе $\{\&, \vee, {}^-\}$ при однотипных константных неисправностях на выходах элементов // Вестник Московского университета. Серия 15. Вычислительная математика и кибернетика. — 2008. — № 1. — С. 40–44.

ОБОБЩЕННЫЙ МЕТОД ОТПЕЧАТКОВ ДЛЯ КВАНТОВЫХ ВЕТВЯЩИХСЯ ПРОГРАММ

А. В. Васильев (Казань)

В данной работе развивается *метод отпечатков* (*fingerprinting*), предназначенный для построения эффективных по памяти квантовых алгоритмов в квантовых моделях вычислений с классическим управлением, таких как *упорядоченные один раз читающие квантовые ветвящиеся программы* (*OBDD*) [1, 2].

Ключевым моментом использования предложенного метода является представление вычисляемых булевых функций *характеристическими полиномами.*

Определение 1. *Назовем полином g_f над некоторым кольцом вычетов $\mathbb{Z}_m$ характеристическим для булевой функции $f(x_1, \ldots, x_n)$, если для любого $\sigma \in \{0,1\}^n$ выполняется:* $f(\sigma) = 1 \iff g_f(\sigma) = 0$.

Такой полином существует для каждой булевой функции f — его можно построить по произвольной ДНФ для отрицания f следующими заменами:

$$x_i \to x_i$$

$$\overline{x}_i \to (1 - x_i)$$

$$\vee \to +$$

$$\& \to \cdot$$

Однако, это не единственный способ получить характеристический полином, и нам требуется выбрать тот, что обладает нужным свойством, а именно — линейностью.

Доказана следующая теорема.

Теорема 1. *Если для булевой функции $f(x_1, \ldots, x_n)$ существует линейный характеристический полином g_f над $\mathbb{Z}_m$, т.е. $g_f = c_1x_1 + \ldots c_nx_n + c_0$, то f может быть вычислена квантовой OBDD ширины $O(\log m)$.*

Указанный подход демонстрируется на некоторых индивидуальных функциях, в основе которых лежит проверка равенства.

1. MOD_m. Функция MOD_m проверяет, кратно ли число единиц во входном наборе параметру m. Линейный полином над $\mathbb{Z}_m$ выбран следующим образом:

$$\sum_{i=1}^{n} x_i.$$

2. MOD'_m. Эта функция отличается от MOD_m только тем, что входной набор интерпретируется как двоичное число. Поэтому для данной функции можно использовать следующий полином над $\mathbb{Z}_m$:

$$\sum_{i=1}^{n} x_i 2^{i-1}.$$

3. EQ_n. Функция EQ_n проверяет равенство двух n-битных двоичных наборов и может задаваться следующим полиномом над $\mathbb{Z}_{2^n}$:

$$\sum_{i=1}^{n} x_i 2^{i-1} - \sum_{i=1}^{n} y_i 2^{i-1}.$$

4. $Palindrome_n(x_1, \ldots, x_n). \equiv \left[x_1 x_2 \ldots x_{\lfloor n/2 \rfloor} = x_n x_{n-1} \ldots x_{\lceil n/2 \rceil + 1}\right]$. Для данной функции существует следующий полином над $\mathbb{Z}_{2^n}$:

$$\sum_{i=1}^{\lfloor n/2 \rfloor} x_i 2^{i-1} - \sum_{i=\lceil n/2 \rceil}^{n} x_i 2^{n-i}$$

5. $PERM_n$. Эта функция проверяет, является ли булевская $n \times n$ матрица перестановочной, т.е. содержащей ровно одну единицу в каждой строчке и каждом столбце. Для данной функции существует следующий линейный полином над $\mathbb{Z}_{(n+1)^{2n}}$:

$$\sum_{i=1}^{n} \sum_{j=1}^{n} x_{ij} \left((n+1)^{i-1} + (n+1)^{n+j-1}\right) - \sum_{i=1}^{2n} (n+1)^{i-1}.$$

Для описанных функций в таблице приводятся нижние оценки сложности (ширины) реализации в детерминированных OBDD и получаемые по нашему методу верхние оценки сложности представления в квантовых OBDD.

	OBDD	QOBDD
MOD_m	$\Omega(m)$	$O(\log m)$
MOD'_m	$\Omega(m)$	$O(\log m)$
EQ_n	$2^{\Omega(n)}$	$O(n)$
$Palindrome_n$	$2^{\Omega(n)}$	$O(n)$
$PERM_n$	$\Omega(2^n n^{-1/2})$	$O(n \log n)$

Возможно следующее обобщение нашего подхода. Вводится определение *характеристики* булевой функции.

Определение 2. *Назовем множество χ_f^m полиномов над $\mathbb{Z}_m$ характеристикой булевой функции f, если для всех $g \in \chi_f^m$ и всех $\sigma \in \{0,1\}^n$ выполняется: $f(\sigma) = 1 \iff g(\sigma) = 0$.*

Мы называем характеристику *линейной*, если все ее элементы линейны. Теорема 1 обобщается следующим образом

Теорема 2. *Если χ_f^m есть линейная характеристика f, то f может быть вычислена квантовой OBDD ширины $O(2^{|\chi_f^m|} \log m)$.*

Обобщенный подход позволил построить эффективную по памяти квантовую ветвящуюся программу, вычисляющую булевский вариант *задачи о скрытой подгруппе*.

Работа выполнена при финансовой поддержке РФФИ, проекты 08-07-00449-а и 09-01-97004-р-поволжье-а.

Список литературы

1. Аблаев Ф. М., Васильев А. В. О вычислениях в квантовых ветвящихся программах методом "характерных признаков" // Материалы XV Международной конференции "Проблемы теоретической кибернетики" (Казань, Россия, 27 июня, 2008). — Казань: Изд-во "Отечество", 2008. — С. 1.

2. Ablayev F., Vasiliev A. On the Computation of Boolean Functions by Quantum Branching Programs via Fingerprinting // Electronic Colloquium on Computational Complexity, 2008. — TR08–059.

НЕОБХОДИМЫЕ И ДОСТАТОЧНЫЕ УСЛОВИЯ РЕАЛИЗАЦИИ БУЛЕВЫХ ФУНКЦИЙ АСИМПТОТИЧЕСКИ ОПТИМАЛЬНЫМИ СХЕМАМИ С НЕНАДЕЖНОСТЬЮ 2ε

А. В. Васин (Пенза)

Рассматривается реализация булевых функций схемами из ненадежных функциональных элементов в полном базисе $B \subseteq B_3$ (B_3 — множество всех булевых функций, зависящих от переменных x_1, x_2, x_3). Предполагается, что все элементы схемы независимо друг от друга с вероятностью ε ($\varepsilon \in (0; 1/2)$) подвержены инверсным неисправностям на выходах. Эти неисправности характеризуются тем, что в исправном состоянии функциональный элемент реализует приписанную ему булеву функцию e, а в неисправном — функцию $\bar{e}$. Считаем, что схема S из ненадежных элементов реализует булеву

функцию $f(x_1, x_2, \ldots, x_n)$, если при поступлении на входы схемы набора $\tilde{a} = (a_1, a_2, \ldots, a_n)$ при отсутствии неисправностей в схеме на ее выходе появляется значение $f(\tilde{a})$. Обозначим $P_{\overline{f(\tilde{a})}}(S, \tilde{a})$ — вероятность ошибки на входном наборе $\tilde{a}$ схемы S, реализующей функцию f. Число $P(S) = \max\limits_{\tilde{a}} P_{\overline{f(\tilde{a})}}(S, \tilde{a})$ назовем ненадежностью схемы S. Надежность схемы S равна $1 - P(S)$.

Пусть $P_\varepsilon(f) = \inf\limits_S P(S)$, где ε — вероятность инверсной неисправности на выходе одного элемента, а инфимум берется по всем схемам S из ненадежных элементов, реализующим функцию $f(x_1, x_2, ..., x_n)$. Схема A из ненадежных элементов, реализующая функцию f, называется асимптотически оптимальной по надежности, если $P(A) \sim P_\varepsilon(f)$ при $\varepsilon \to 0$, т. е. $\lim\limits_{\varepsilon \to 0} \frac{P_\varepsilon(f)}{P(A)} = 1$.

В работах [1] и [2] найдено множество функций $G = G_1 \cup G_2 \cup G_3$, зависящих от переменных x_1, x_2, x_3, где G_1 – множество функций, конгруэнтных одной из функций $x_1^{\sigma_1}x_2^{\sigma_2} \vee x_1^{\sigma_1}x_3^{\sigma_3} \vee x_2^{\sigma_2}x_3^{\sigma_3}$, G_2 — множество функций, конгруэнтных одной из функций $x_1^{\sigma_1}x_2^{\sigma_2} \oplus x_3^{\sigma_3}$, G_3 — множество функций, конгруэнтных одной из функций $x_1^{\sigma_1}x_2^{\bar{\sigma}_2} \vee x_2^{\sigma_2}x_3^{\sigma_3}$, где $\sigma_1, \sigma_2, \sigma_3 \in \{0, 1\}$. Обозначим B_3 — множество всех функций, зависящих от переменных x_1, x_2, x_3.

В работах [3] и [4] выделено множество функций $M = M_1 \cup M_2 \cup M_3 \cup M_4 \cup M_5 \cup M_1^* \cup M_2^* \cup M_3^* \cup M_4^*$, зависящих от переменных x_1, x_2, x_3, где M_1 — множество функций, конгруэнтных одной из функций $x_1^{\sigma_1}x_2^{\sigma_2} \vee x_1^{\bar{\sigma}_1}x_2^{\bar{\sigma}_2}x_3^{\bar{\sigma}_3}$, M_2 — множество функций, конгруэнтных одной из функций $x_1^{\sigma_1}x_2^{\sigma_2}x_3^{\sigma_3} \vee x_1^{\sigma_1}x_2^{\bar{\sigma}_2}x_3^{\bar{\sigma}_3} \vee x_1^{\bar{\sigma}_1}x_2^{\sigma_2}x_3^{\bar{\sigma}_3}$, M_3 — множество функций, конгруэнтных одной из функций $\bar{x}_1(x_2^{\sigma_2} \vee x_3^{\sigma_3})$, M_4 — множество функций, конгруэнтных одной из функций $x_1^{\sigma_1}x_2^{\sigma_2}x_3^{\sigma_3} \vee x_1^{\bar{\sigma}_1}x_2^{\bar{\sigma}_2}x_3^{\bar{\sigma}_3}$, $M_5 = \{x_1 \oplus x_2 \oplus \sigma_1, x_1 \oplus x_2 \oplus x_3 \oplus \sigma_1\}$ $(\sigma_1, \sigma_2, \sigma_3 \in \{0, 1\})$ и множества M_1^*, M_2^*, M_3^*, M_4^* — множества функций, двойственных соответственно функциям множеств M_1, M_2, M_3, M_4.

Пусть $K_1(n)$ — множество булевых функций $f(x_1, x_2, \ldots, x_n)$, не представимых в виде $(x_i^a \& h(\tilde{x}))^b$ или $(x_i^a \& x_j^b \vee x_i^{\bar{a}} \& x_j^{\bar{b}} \& h(\tilde{x}))^c$, где $h(\tilde{x})$ — произвольная функция, $i, j \in \{1, 2, \ldots, n\}$, $a, b, c \in \{0, 1\}$. Пусть $K_2(n)$ — множество булевых функций $f(x_1, x_2, \ldots, x_n)$, не представимых в виде $(x_i^a \& h(\tilde{x}))^b$ или $((x_i \oplus x_j)^a \cdot h(\tilde{x}))^b$, где $h(\tilde{x})$ — произвольная функция, $i, j \in \{1, 2, \ldots, n\}$, $a, b \in \{0, 1\}$.

Пусть Ψ $(\Psi \subseteq B_3)$ — множество функций, конгруэнтных одной из функций $x_1^{\sigma_1}x_2^{\sigma_2}$, $x_1^{\sigma_1}x_2^{\sigma_2}x_3^{\sigma_3}$, $x_1^{\sigma_1}(x_2^{\sigma_2}x_3^{\sigma_3} \vee x_2^{\bar{\sigma}_2}x_3^{\bar{\sigma}_3})$, $x_1(x_2^{\sigma_2} \vee x_3^{\sigma_3})$

$(\sigma_1, \sigma_2, \sigma_3 \in \{0,1\})$, Ψ^* — множество функций, двойственных функциям множества Ψ, а $\tilde{\Psi}$ — множество функций $B_3 \backslash (G \cup M)$.

Пусть Θ ($\Theta \subseteq B_3$) — множество функций конгруэнтных функциям $x_1^a x_2^b$, $x_1^a x_2^b x_3^c$, $x_1^a (x_2 \oplus x_3)^b$, где $a, b, c \in \{0,1\}$. Θ^* — множество функций, двойственных функциям множества Θ.

Теорема 1 [2]. *Пусть $\varepsilon \in (0, 1/4]$, функция $f(\tilde{x}) \in K_1(n)$, а S — любая схема в полном базисе $B_3 \backslash G$, реализующая функцию f. Тогда $P(S) \geq 2\varepsilon - 2\varepsilon^2$.*

Теорема 2. *Пусть $\varepsilon \in (0, 1/960]$, и полный базис B ($B \subseteq B_3 \backslash G$) удовлетворяет хотя бы одному из следующих условий:*

1) *$B \cap M \neq \varnothing$;*

2) *B содержит функцию $\varphi(x_1, x_2, x_3)$, конгруэнтную одной из функций $x_1(x_2^{\sigma_2} \vee x_3^{\sigma_3})$ ($\sigma_2, \sigma_3 \in \{0,1\}$), и $B \cap \Psi^* \neq \varnothing$;*

3) *B содержит функцию $\varphi^*(x_1, x_2, x_3)$, конгруэнтную одной из функций $x_1 \vee x_2^{\sigma_2} x_3^{\sigma_3}$ ($\sigma_2, \sigma_3 \in \{0,1\}$), и $B \cap \Psi \neq \varnothing$.*

Тогда произвольную булеву функцию f в базисе B можно реализовать такой схемой S, что $P(S) \leq 2\varepsilon + 204\varepsilon^2$.

Из теорем 1 и 2 следует, что в указанных базисах для почти всех булевых функций (поскольку $\frac{|K_1(n)|}{2^{2^n}} \to 1$ с ростом n) асимптотически оптимальные по надежности схемы функционируют с ненадежностью, асимптотически равной 2ε при $\varepsilon \to 0$.

Теорема 3. *Пусть $\varepsilon \in (0, 1/960]$, и полный базис B ($B \subseteq \tilde{\Psi}$) удовлетворяет хотя бы одному из следующих условий:*

1) *$B \subseteq (\Theta \cup \Theta^* \cup \{\bar{x}_1, 0, 1\})$;*

2) *$B \subseteq (\Psi \cup \{\bar{x}_1, 0, 1\})$;*

3) *$B \subseteq (\Psi^* \cup \{\bar{x}_1, 0, 1\})$.*

Тогда любая схема S, реализующая булеву функцию $f(\tilde{x}) \in K_2(n)$, функционирует с ненадежностью $P(S) \geq 3\varepsilon(1-\varepsilon)^3$.

Из теоремы 3 следует, что других базисов в $B_3 \backslash G$, кроме удовлетворяющих условиям теоремы 2, в которых бы асимптотически оптимальные по надежности схемы для почти всех функций функционировали с ненадежностью 2ε ($\varepsilon \to 0$), нет.

Список литературы

1. Васин А. В. О функциях специального вида // Труды VIII международной конференции "Дискретные модели в теории управляющих систем" — М.: МАКС Пресс, 2009. — С. 43–46.

2. Алехина М. А., Васин А. В. О надежности схем в базисах, содержащих функции не более чем трех переменных // Ученые

записки Казанского государственного университета. Сер. Физико-математические науки. — 2009. — Т. 151, кн. 2. — С. 25–36.

3. Алехина М. А., Васин А. В. Достаточные условия реализации булевых функций асимптотически оптимальными схемами с ненадежностью 2ε // Известия высших учебных заведений. Математика. Казанский государственный университет. — В печати.

4. Васин А. В. Об асимптотически оптимальных схемах в частных базисах, содержащих линейные функции двух или трех переменных // Труды Международной научно-технической конференции "Проблемы автоматизации и управления в технических системах" (г. Пенза, 20–23 октября 2009 г.) — Пенза: Изд-во ПГУ, 2009. — С. 48–50.

О ПРЕДСТАВИМОСТИ ЯЗЫКОВ В ОДНОСТОРОННИХ k-ГОЛОВОЧНЫХ АВТОМАТАХ, РАБОТАЮЩИХ В РЕАЛЬНОЕ ВРЕМЯ

Р. Р. Гараев (Казань)

Рассматривается автоматная сложность языков, определяемая на основе известного отношения Майхилла—Нероуда.

Пусть $L \subseteq X^*$ — произвольный язык над алфавитом X. Для слова $u \in X^*$ определим множество $L_n(u) = \{r : |r| \leq n \text{ и } ur \in L\}$.

Определение. Два слова u и v будем называть *n-эквивалентными* относительно языка L (и писать $u \equiv_L^n v$) тогда и только тогда, когда $L_n(u) = L_n(u')$.

Через $\varphi_L(n)$ будем обозначать число классов n-эквивалентности относительно языка L. Будем называть это число *n-рангом языка* L, $\varphi_L(n)$ является характеристикой автоматной сложности языка.

Поведение функции $\varphi_L(n)$ для различных языков изучались разными авторами (см., например, [1, 5]). В данной работе развивается коммуникационная техника оценки поведения функций $\varphi_L(n)$. Получены следующие результаты:

1. $ISA = \{w : w = u\sharp r,\ u, r \in \{0,1\}^*,\ u_{N(r)} = 1\}$ — этот язык известен также как "мультиплексорная функция" (см., например, [2]):
$$\varphi_{ISA(n)}(n) = \Theta(2^{2^n}).$$
2. $L_f^p = \{u : u = x^1\sharp x^2\sharp \ldots \sharp x^p 2y,\ y_i = f(x_i^1, x_i^2, \ldots, x_i^p)\}$:
$$\varphi_{L_f^p}(n) = \Theta(2^{pn}).$$
3. $Include = \{w : w = u\sharp v,\ v \text{ является подсловом } u\}$:
$$\varphi_{Include}(n) = \Theta(2^{2^n}).$$

Через $\mathcal{L}(k-DFA)$ обозначим класс языков, представимых в односторонних k-головочных детерминированных автоматах, работающих в реальное время. Известна иерархия [6]:

$$\mathcal{L}(k-DFA) \subsetneq \mathcal{L}((k+1)-DFA).$$

В данной работе с применением нашей техники дается простое и прозрачное доказательство этой иерархии. Содержательно доказательство строится следующим образом: k-головочный автомат интерпретируется как специального вида бесконечный детерминированный автомат (БДА).

Известно, что любой язык $L \subseteq X^*$ представим в подходящем БДА $A = \langle X, S, \delta, s_0, F\rangle$ с начальным состоянием s_0 и финальным множеством состояний F.

Для состояний БДА A определим множество:

$$F_n(s) = \{r : |r| \leq n \text{ и } \delta(s,r) \in F\}.$$

Два состояния s и s' бесконечного детерминированного автомата A будем называть *n-эквивалентными* (и писать $s \equiv_A^n s'$) тогда и только тогда, когда выполняется $F_n(s) = F_n(s')$.

Через $\pi_A(n)$ обозначим число различных классов n-эквивалентности. Будем называть это число *пропускной способностью автомата.*

Известно, что если язык L представим в БДА A, тогда выполняется

$$\varphi_L(n) \leq \pi_A(n).$$

Введем следующие обозначения: $\mathcal{L}(k-DFA)$ — класс языков, распознаваемых k-головочными односторонними детерминированными автоматами, работающими в реальное время; $\mathcal{L}(k-NFA)$ — класс языков, распознаваемых k-головочными односторонними недетерминированными автоматами, работающими в реальное время.

Работу k-головочного одностороннего автомата можно промоделировать в виде подходящего БДА. При этом пропускная способность $\pi_A(n)$ оценивается следующим образом:

1. Пропускная способность k-головочных односторонних детерминированных автоматов, работающих в реальное время:

$$\pi_{k-DFA}(n) = \Theta(2^{(k-1)n}).$$

2. Пропускная способность k-головочных односторонних недетерминированных автоматов, работающих в реальное время:

$$\pi_{k-NFA}(n) = \Theta(2^{2^{(k-1)n}}).$$

Известна иерархия языков по количеству головок:

$$\pounds(k-DFA) \subsetneq \pounds((k+1)-DFA).$$

Эту иерархию несложно доказать, используя нашу технику. На примере языка $L_\vee^k$:

1. Нами построен алгоритм для $(k+1)$-головочного автомата. Из этого следует $L_\vee^k \in \mathcal{L}((k+1)-DFA)$.

2. $L_\vee^k \notin \mathcal{L}(k-DFA)$. Это следует из

$$\varphi_{L_\vee^k}(n) = \Theta(2^{kn}) \succeq \Theta(2^{(k-1)n}) = \pi_A(n).$$

Недетерминированные модели сильнее детерминированных моделей. Имеет место следующий результат:

$\mathcal{L}(2-NFA) \setminus \mathcal{L}((k)-DFA) \neq \varnothing$ для любого $k = const$.

Язык $Include \in \mathcal{L}(2-NFA) \setminus \mathcal{L}((k)-DFA)$. Это следует из того, что:

1. Можно построить недетерминированный алгоритм для распознавания этого языка двухголовочным конечным недетерминированным автоматом, работающим в реальное время.

2. Для любого $k = const$ найдется такое n, что $\varphi_{Include}(n) = \Theta(2^{2^n}) \succeq 2^{kn}$.

Список литературы

1. Аблаев Ф. М. Возможности вероятностных и недетерминированных машин по представлению языков в реальное время // Дисс. ... канд. физ.-мат. наук. — 1982.

2. Ложкин С. А., Власов И. В. О сложности мультиплексорной функции в классе π-функций // Ученые записки Казанского государственного университета. —2009. — Т. 2. — С. 98–106.

3. Фрейвалд Р. В. Возможности различных моделей односторонних вероятностных автоматов // Известия ВУЗов. Сер. Математика. — 1981. — № 5 (228).

4. Ablayev F. M. Lower bounds for one-way probabilistic communication complexity and their application to space complexity // Theor. Comput. Sci. — 1996. — V. 2 157. — P. 139–159.

5. Chrobak M. Hierarchies of one-way multihead automata languages // Proc. ICALP'85. — Lecture Note in Computer Science. — V. 194.

6. Yao A. C., Rivest R. L. k+1 heads are better than k // Journal of ACM. — 1978. — V. 25. — P. 337–340.

О СЛОЖНОСТИ БУЛЕВЫХ ЛИНЕЙНЫХ ОПЕРАТОРОВ С РЕДКИМИ МАТРИЦАМИ

С. Б. Гашков, И. С. Сергеев (Москва)

Пусть A — булева матрица. Обозначим через $L_{\oplus}(A)$ сложность реализации соответствующего матрице линейного оператора схемами из функциональных элементов над базисом $\{\oplus\}$. Аналогично через $L_{\vee}(A)$ обозначим сложность реализации определяемой данной матрицей системы дизъюнкций.

В работе Б. С. Митягина и Б. Н. Садовского [1] фактически был поставлен вопрос о величине

$$\lambda(n) = \max_{M_n} \frac{L_{\vee}(M_n)}{L_{\oplus}(M_n)},$$

где M_n — матрица размера $n \times n$, а также о величине $\lambda^*(n)$, определение которой отличается от $\lambda(n)$ тем, что рассматриваются только матрицы без прямоугольников, т. е. матрицы, не содержащие подматриц из всех единиц размера 2×2.

Как показано Э. И. Нечипоруком в [2], для матрицы A без прямоугольников $L_{\vee}(A) = \nu(A) - n$, где $\nu(A)$ — вес матрицы, а n — число ненулевых строк в ней (в дальнейшем будем, без ограничения общности, полагать, что рассматриваемые матрицы не содержат ненулевых строк). В общем случае величина $\nu(A) - n$ играет роль сложности наивной реализации оператора с матрицей A, когда все его компоненты реализуются независимо. Введем также величину

$$\lambda^v(n) = \max_{M_n} \frac{\nu(M_n) - n}{L_{\oplus}(M_n)},$$

где M_n — матрица размера $n \times n$ без повторяющихся строк.

Теорема.

(1) $\Theta\left(\frac{\sqrt{n}}{\log n \log\log n}\right) \le \lambda^*(n) = O(\sqrt{n})$, *причем можно явно указать матрицу, на которой достигается нижняя оценка;*

(2) $\Theta\left(\frac{n}{\log^{O(1)} n}\right) \le \lambda(n) = O\left(\frac{n}{\log n}\right)$, *при этом можно явно указать матрицу, для которой соответствующее отношение по порядку равно* $\frac{n}{c\sqrt{\log n \log\log n}}$;

(3) $\lambda^v(n) \sim (2 - \sqrt{2})n$.

Для доказательства асимптотического равенства (3) достаточно рассмотреть матрицу максимального веса, для которой соответ-

ствующий оператор реализуется схемой сложности αn, и затем подобрать оптимальное значение α.

Верхняя оценка (1) вытекает из известной оценки $\Theta(n^{3/2})$ веса матрицы порядка n без прямоугольников. Верхняя оценка (2) вытекает из принадлежащей О. Б. Лупанову [3] оценки $L_\vee(M_n) = O(n^2/\log n)$. При этом случай операторов малой сложности в обоих пунктах рассматривается отдельно.

Центральным вопросом является получение нижних оценок для величин $\lambda(n)$ и $\lambda^*(n)$.

В работе [1] было предложено доказательство того, что $\lambda^*(n) = \Omega\left(n^{1/2-o(1)}\right)$, которое, однако, оказалось неверным. В последующих работах удавалось оценить $\lambda^*(n)$ снизу только константой. При этом, однако, были получены близкие двусторонние оценки для представляющей самостоятельный интерес величины $\lambda_3^*(n)$, определение которой отличается от определения $\lambda^*(n)$ тем, что рассматриваются схемы глубины 3 (и только матрицы, реализуемые такими схемами). А именно, было доказано $2 \geq \lambda_3^*(n) \geq 12/7 - o(1)$ (верхняя оценка — первым автором в 1973 г. в курсовой работе, нижняя оценка — К. А. Зыковым в работе [4]).

В действительности, для доказательства нижних оценок (1) и (2) достаточно рассмотреть циркулянтные матрицы (строки циркулянтной матрицы получаются последовательными циклическими сдвигами). Определяемый циркулянтной матрицей Z_n порядка n линейный оператор есть оператор умножения на константу в кольце $GF(2)[x]/(x^n+1)$, поэтому $L_\oplus(Z_n) = O(n \log n \log\log n)$, если воспользоваться методом Шёнхаге [5].

Чтобы завершить доказательство (1), остается предъявить циркулянтную матрицу без прямоугольников веса $\Theta(n^{3/2})$. Для этой цели подойдет матрица Зингера — пример из работы [1].

Нижняя оценка (1) достигается также и на матрице Нечипорука [2], которая фактически является матрицей дискретного преобразования Фурье порядка p в кольце $GF(2)[x]/(x^p+1)$, где p — простое число.

Нижняя оценка (2) вытекает из установленного М. И. Гринчуком [6] факта существования циркулянтной матрицы Z_n порядка n, для которой $L_\vee(Z_n) \geq \Theta\left(n^2/\log^{O(1)} n\right)$. Метод [6] однако не позволяет указать явно матрицу, на которой достигается эта оценка.

Для получения несколько более слабой, но конструктивной нижней оценки можно взять матрицу R_n из работы [7], которая опреде-

ляется следующим образом. Пусть $n = p^t$, где p — простое число. Занумеруем строки и столбцы матрицы элементами поля $GF(p^t)$. На пересечении строки x и столбца y матрицы R_n стоит единица в том и только том случае, когда $(x-y)^{(p^t-1)/(p-1)} = 1$. Эта матрица определяет оператор умножения на некоторую константу в кольце $GF(2)[x_1, \ldots, x_t]/(x_1^p+1, \ldots, x_t^p+1)$. Модифицировав метод Шёнхаге, можно показать, что такое умножение выполняется со сложностью $O(2^t n \log n \log\log n)$.

При подходящем выборе параметров p и t для матрицы R_n оценка $\frac{L_\vee(R_n)}{L_\oplus(R_n)} \geq \Theta\left(\frac{n}{c^{\sqrt{\log n \log\log n}}}\right)$ устанавливается сопоставлением следующих двух фактов. Матрица R_n не содержит подматриц размера $t \times (t!+1)$ и размера $(t!+1) \times t$ из всех единиц [7]. Если матрица A порядка n не содержит подматриц размера $s \times t$ из всех единиц (такие матрицы мы называем *редкими*), то $L_\vee(A) \geq \Theta\left(\frac{\nu(A)-n}{st}\right)$ (Мельхорн [8]).

Работа выполнена при финансовой поддержке РФФИ (проекты 08–01–00863 и 08–01–00632), программы поддержки ведущих научных школ РФ (проект НШ–4437.2010.1) и программы фундаментальных исследований ОМН РАН «Алгебраические и комбинаторные методы математической кибернетики и информационные системы нового поколения».

Список литературы

1. Митягин Б. С., Садовский Б. Н. О линейных булевских операторах // Доклады АН СССР. — 1965. — Т. 165 (4). — С. 773–776.

2. Нечипорук Э. И. Об одной булевской матрице // Проблемы кибернетики. Вып. 21. — М.: Наука, 1969. — С. 237–240.

3. Лупанов О. Б. О вентильных и контактно-вентильных схемах // Доклады АН СССР. — 1956. — Т. 111 (6). С. 1171–1174.

4. Зыков К. А. О сложности реализации линейных булевых преобразований схемами глубины три // Вестник МГУ. Математика. Механика. — 1998. — №2. — С. 68–70.

5. Schönhage A. Schnelle multiplikation von polynomen über körpern der charakteristik 2 // Acta Inf. — 1977. — V. 7. — P. 395–398.

6. Гринчук М. И. О сложности реализации циклических булевых матриц вентильными схемами // Изв. Вузов. Математика. — 1988. — Т. 7. — С. 39–44.

7. Kóllar J., Rónyai L., Szabó T. Norm-graphs and bipartite Turán numbers // Combinatorica. — 1996. — V. 16, № 3. — P. 399–406.

8. Мельхорн К. Некоторые замечания, касающиеся булевых сумм // Киберн. сборник. Вып. 18. — М.: Мир, 1981. — С. 39–45.

ЧАСТНЫЙ СЛУЧАЙ ЗАДАЧИ О РАЗБИЕНИИ МНОЖЕСТВА, ДОПУСКАЮЩИЙ КВАДРАТИЧНУЮ ВРЕМЕННУЮ СЛОЖНОСТЬ НА ДЕТЕРМИНИРОВАННОЙ МАШИНЕ ТЬЮРИНГА

М. А. Герасимов (Санкт-Петербург)

Рассматривается применение алгоритма Хаффмана к решению NP-полной задачи о разбиении множества элементов с целыми неотрицательными весами на два дизъюнктных, равных по весу подмножества. Предлагается специальный метод сведения данной задачи к задаче кодирования оптимальным кодом. Предлагаемый метод дает приближенное решение задачи о разбиени [1]. Рассматривается случай, когда предлагаемый подход дает точное решение этой задачи за квадратичное время на одноленточной машине Тьюринга.

Детерминированная машина Тьюринга. Для анализа алгоритма рассматривается одноленточная, одноголовочная машина Тьюринга со входной и выходной лентой. Предполагается, что входные данные записаны на входной ленте, обрабатываются на рабочей ленте и результат записывается на выходной ленте. При работе машины Тьюринга используется алфавит, состоящий из четырех символов $\{\#, b, 0, 1\}$. Результатом работы алгоритма считается битовая последовательность, кодирующая исходные данные и соответствующее дерево кодирования, позволяющее однозначно восстановить исходную последовательность. В дальнейшем будем считать, что входные данные (натуральные числа) записаны в виде битовой последовательности на входной ленте между двумя маркерами '#'. В качестве разделителей используется пустой символ 'b'. Считывание второго маркера означает конец цепочки входных данных. Входная лента позволяет считывать входные данные произвольное количество раз. Выходная лента позволяет только записывать результат вычисления в виде последовательности символов рабочего алфавита. Каждый символ выходной цепочки записывается только один раз и больше не изменяется.

Сведение задачи о разбиении к задаче поиска оптимального кода. Рассматриваемая реализация алгоритма Хаффмана использует линейный список входных элементов, занумерованных натуральными числами $X = \{x_1, , x_M\}$ и имеющих положительные веса $\{w_1, , w_M\}$ соответственно. Обозначим через $W(X)$ суммарный вес элементов множества X:

$$W(X) = \sum_{i=1}^{M} w_i.$$

Пусть множество X разбито на K дизъюнктных подмножеств, $K \geq 2, X_1, X_2, ..., X_K : X_i \cap X_j = \oslash$, $X_1 \cup X_2 ... \cup X_K = X$. Согласно [1] весом разбиения назовем величину

$$F(X_1, X_2, ..., X_K) = \max\{W(X_1), W(X_2), ..., W(X_K)\}$$

Требуется найти такое разбиение множества X на K подмножеств $X_1^*, X_2^*, ..., X_K^*$, что

$$F(X_1^*, X_2^*, ..., X_K^*) = \min\{F(X_1, X_2, ..., X_K)\}$$

Нахождение разбиения $\{X_1^*, X_2^*, ... X_K^*\}$ множества X и точного значения $F(X_1^*, X_2^*, ..., X_K^*)$ для заданного множества элементов X является NP-полной задачей [2]. Одним из направлений исследования возможностей приближенного решения этой задачи за полиномиальное время на детерминированной машине Тьюринга является поиск решения $F(X_1, X_2, ..., X_K)$, достаточно близкого к $F(X_1^*, X_2^*, ..., X_K^*)$ за полиномиальное время. Данная работа относится к этой области. Предлагается сведение этой задачи к задаче оптимального кодирования: вместо весов $\{w_1, , w_M\}$ предлагается рассматривать относительные веса элементов $\{v_1, , v_M\}$, которые могут вычисляться по формуле:

$$v_i = \frac{w_i}{\sum_{i=1}^{M} w_i}.$$

В этом случае:

$$\sum_{i=1}^{M} v_i = 1$$

и к данному набору элементов $X = \{x_1, , x_M\}$ можно применить алгоритм Хаффмана с алфавитом из K букв, рассматривая v_i как частоту i-го элемента. В полученном кодовом дереве в качестве множества X_1 нужно взять все листья первого главного поддерева, в качестве множества X_2 — листья второго главного поддерева, ..., в качестве множества X_K — листья K-го главного поддерева.

Частный случай задачи о разбиении.

Теорема. *Пусть входной поток данных содержит* $X = \{x_1, , x_M\}$ *различных элементов с весами* $\{w_1, , w_M\}$. *Относительные веса этих элементов* $v_i = K^{-m_i}$, *где* $K \geq 2, m_i \geq 1$; K, m_i — *целые. Тогда дерево кодирования данных элементов алгоритмом Хаффмана в алфавите из* K *букв является деревом кодирования*

этих же элементов алгоритмом Шеннона—Фано в этом же алфавите.

Следствие. *Дерево кодирования методом Шеннона—Фано дает решение задачи о разбиении множества* $X = \{x_1, , x_M\}$ *на* K *дизъюнктных подмножеств с одинаковыми весами. Поэтому, в том случае, когда относительные веса элементов* $\{v_1, , v_M\}$ *разбиваемого множества равны* K^{-m_i}, *где* $K \geq 2, m_i \geq 1$; K, m_i — *целые, задача о разбиении на* K *дизъюнктных подмножеств может быть точно решена не более чем за квадратичное время от длины входных данных на одноленточной детерминированной машине Тьюринга.*

Список литературы

1. Гэри М., Джонсон Д. Вычислительные машины и труднорешаемые задачи. — М.: Мир, 1982.

2. Fischetti M., Martello S. Wost–case analysis of the differencing method for the partition problem // Math. Programming. — 1987. — V. 37, № 1. — P. 117–120.

3. Минский М. Вычисления и автоматы. — М., 1971.

4. Huffman. D. A method for construction of minimum redundancy codes // Proceeding of IRE. — 1952. — V. 40 (9). — P. 1098–1101.

5. Horowits E., Sahni S. Fundamentals of Computer Algorithms. — Computer Science Press, 1978.

6. Shannon C. E. A mathematical theory of communication // Bell System Technical Journal. — 1848. — V. 27. — P. 373–423.

О СЛОЖНОСТИ РЕАЛИЗАЦИИ ПСЕВДОЛИНЕЙНЫХ ФУНКЦИЙ СПЕЦИАЛЬНОГО ВИДА

Д. А. Дагаев (Москва)

Рассматривается задача о сложности реализации функций многозначной логики формулами над конечными базисами.

О. Б. Лупанов для любой конечной полной системы булевых функций получил асимптотически точную формулу для соответствующей функции Шеннона [1]. А. Б. Угольников показал, что для произвольной конечной системы булевых функций всякая функция из замыкания этой системы может быть реализована формулой со сложностью, имеющей не более чем экспоненциальный порядок роста от числа переменных [2]. Для некоторых полных систем функций k-значной логики в работах [3, 4] найдены асимптотически точные

формулы для соответствующих функций Шеннона. Пример последовательности функций 4-значной логики, сложность которых в классе формул над некоторой конечной неполной системой имеет порядок роста "двойной экспоненты" от числа переменных, приведен в [5]. Все необходимые определения можно найти в [1–7].

В данной работе рассматриваются функции трехзначной логики, принимающие значения 0 или 1; множество всех таких функций обозначается через $P_{3,2}$. Пусть $f(x_1, ..., x_n) \in P_{3,2}$. Проекцией функции f называется такая булева функция $prf(x_1, ..., x_n)$, значение которой на произвольном наборе $\widetilde{\alpha} \in \{0,1\}^n$ определяется равенством $prf(\widetilde{\alpha}) = f(\widetilde{\alpha})$. Проекцией prF множества $F \subseteq P_{3,2}$ называется множество $\bigcup\{prf\}$, где объединение берется по всем $f \in F$. Положим $\mathcal{L} = \{f \in P_{3,2} | prf \in L\}$, где L — множество всех линейных булевых функций. Функция $f \in P_{3,2}$ называется псевдолинейной, если $f \in \mathcal{L}$. Множество всех замкнутых классов псевдолинейных функций описано в [6]. В данной работе усиливается результат из [7].

Определим некоторые функции из $P_{3,2}$. Через $j_i(x)$, $i \in \{0,1,2\}$, обозначим функцию, равную 1 при $x = i$ и 0 в остальных случаях; через $\lambda(x,y)$ — функцию, равную 1 на наборах $(1,0), (0,1), (1,2), (2,1)$ и 0 в остальных случаях (эту функцию будем также обозначать $x+y$); через $x \cdot y$ — функцию, равную 1 на наборе $(1,1)$ и 0 в остальных случаях. Положим $\mu(x,y) = j_1(x) \cdot j_2(y)$.

Каждая псевдолинейная функция $f(x_1, ..., x_n)$ может быть представлена в виде

$$f(x_1, ..., x_n) = \eta_f(x_1, ..., x_n) + \sum_{I,J} a_{I,J} \varkappa_{I,J}(x_1, ..., x_n), \qquad (1)$$

где $\eta_f(x_1, ..., x_n) = a + a_1 j_1(x_1) + ... + a_n j_1(x_n)$, функция $\varkappa_{I,J}$ является произведением двух множителей, первый из которых является произведением по $i \in I$ функций $j_1(x_i)$, а второй — произведением по $j \in J$ функций $j_2(x_j)$, $a, a_i, a_{I,J} \in \{0,1\}$, и суммирование в (1) производится по всем множествам I, J, таким, что $I \cup J \subseteq \{1, ..., n\}$, $I \cap J = \varnothing$, $J \neq \varnothing$ (см. [6]). Если $a_{I,J} = 1$, то функция $\varkappa_{I,J}$ называется компонентой функции f. Множество всех компонент функции f будем обозначать через K_f. Обозначим через J_f множество всех функций $j_1(x_i)$, $1 \leqslant i \leqslant n$, таких, что $a_i = 1$. Определим множество H_f следующим образом: если $a = 1$, то $H_f = \{1\}$, в противном случае $H_f = \varnothing$. Положим $Y_f = K_f \cup J_f \cup H_f$.

Положим $\mathcal{L}_2 = [\{1, \lambda, \mu\}]$. Пусть $f(x_1, ..., x_n) \in \mathcal{L}_2$, $n \geqslant 1$. Рассмотрим представление функции f в виде (1). Определим множество

$\mathcal{I} = \mathcal{I}(f)$ наборов с натуральными компонентами следующим образом. Набор $\widetilde{i} = (i_1, ..., i_l)$, где $1 \leqslant l \leqslant n$, $l = l(\widetilde{i})$, принадлежит множеству $\mathcal{I}$ тогда и только тогда, когда $1 \leqslant i_1 < ... < i_l \leqslant n$ и выполняется по крайней мере одно из двух условий: $j_2(x_{i_1})...j_2(x_{i_l}) \in K_f$ или $j_1(x_t)j_2(x_{i_1})...j_2(x_{i_l}) \in K_f$ хотя бы для одного $t \in \{1, ..., n\} \setminus \{i_1, ..., i_l\}$.

Обозначим через R_f множество натуральных чисел i, таких, что $1 \leqslant i \leqslant n$ и в множестве $\mathcal{I}(f)$ существует хотя бы один набор, имеющий компоненту, равную i. Положим $r_f = |R_f|$.

Определим индукцией по величине r_f величину $A(f)$, которая однозначно вычисляется по функции $f(x_1, ..., x_n) \in \mathcal{L}_2$, $n \geqslant 1$. Если $r_f = 0$, то положим $A(f) = 0$. Пусть $r_f \neq 0$. Пусть $f_1, ..., f_s$ — такие функции из $\mathcal{L}_2(n)$, что $s \geqslant 1$ и одновременно выполняются следующие условия: 1) для каждого $i = 1, ..., s$ выполняется неравенство $|Y_{f_i}| \geqslant 1$; 2) для каждого $i = 1, ..., s$ найдется переменная x_l, $l = l(i)$, такая, что множитель $j_2(x_l)$ содержится в каждом элементе множества Y_{f_i}; 3) $|Y_{f_i}| \cap |Y_{f_j}| = \varnothing$ для любых $1 \leqslant i < j \leqslant s$; 4) $f = \eta_f + f_1 + ... + f_s$.

Обозначим через $\widetilde{f}_i$ функцию, которая получается из представления функции f_i в виде (1) вынесением за скобки множителя $j_2(x_l)$, $l = l(i)$. Тогда $f_i = \widetilde{f}_i \cdot j_2(x_l)$ и $l \notin R_{\widetilde{f}_i}$, $i = 1, ..., s$. Так как $l \notin R_{\widetilde{f}_i}$, то $r_{\widetilde{f}_i} < r_f$ для всех $i = 1, ..., s$.

Положим $D = \{f_1, ..., f_s\}$. Обозначим через $\mathcal{Z}_f$ множество всех множеств D, удовлетворяющих условиям 1–4. Очевидно, что $\mathcal{Z}_f \neq \varnothing$. Пусть $\mathcal{Z}_f = \{D_1, ..., D_t\}$, $t \geqslant 1$. Для каждого $i = 1, ..., t$ рассмотрим множество $D_i = \{f_{1i}, ..., f_{si}\}$, $s = s(i)$. Положим

$$A_i(f) = (1 + A(\widetilde{f}_{1i})) + ... + (1 + A(\widetilde{f}_{si})) = s + A(\widetilde{f}_{1i}) + ... + A(\widetilde{f}_{si}),$$

где $s = s(i)$. Положим $A(f) = \min A_i(f)$, где минимум берется по всем $i = 1, ..., t$. Имеет место следующая

Теорема. *Пусть $f(x_1, ..., x_n)$ — функция из класса $\mathcal{L}_2$, существенно зависящая не менее чем от двух переменных. Тогда*

$$L_{\mathfrak{C}}(f) = |Y_f| + A(f).$$

Автор выражает благодарность профессору А. Б. Угольникову за постоянное внимание к работе.

Работа выполнена при финансовой поддержке РФФИ (проект 08–01–00863), программы поддержки ведущих научных школ РФ

(проект НШ–4437.2010.1) и программы фундаментальных исследований ОМН РАН «Алгебраические и комбинаторные методы математической кибернетики и информационные системы нового поколения».

Список литературы

1. Лупанов О. Б. О сложности реализации функций алгебры логики формулами // Проблемы кибернетики. Вып. 3. — М.: Физматгиз, 1960. — С. 61–80.

2. Угольников А. Б. О глубине формул в неполных базисах // Математические вопросы кибернетики. Вып. 1. — М.: Наука, 1988. — С. 242–245.

3. Захарова Е. Ю. Реализация функций из P_k формулами // Матем. заметки. — 1972. — Т. 11, № 1. — С. 99–108.

4. Гашков С. Б. О параллельном вычислении некоторых классов многочленов с растущим числом переменных // Вестн. Моск. Ун-та. Матем. Механ. — 1990. — № 2. — С. 88–92.

5. Угольников А. Б. О сложности реализации формулами одной последовательности функций 4-значной логики // Вестн. Моск. Ун-та. Матем. Механ. — 2004. — № 3. — С. 52–55.

6. Lau D. Function Algebras on Finite Sets. — Berlin: Springer-Verlag, 2006.

7. Дагаев Д. А. Об одном классе псевдолинейных функций // Мат-лы XVIII Международной школы-семинара "Синтез и сложность управляющих систем" (Пенза, 28 сентября – 3 октября 2009 г.). — М.: Изд-во мех.-мат. ф-та МГУ, 2009. — С. 31–33.

ДВА СООБЩАЮЩИХСЯ ПЕРЕКРЕСТКА КАК ДИСКРЕТНАЯ УПРАВЛЯЮЩАЯ СИСТЕМА

А. В. Зорин (Нижний Новгород)

В работах [1, 2] предлагается новый подход к построению математической модели управляющей системы обслуживания с общей позиции управляющей (кибернетической) системы [3]. В данной статье этот подход применяется к построению модели управления по циклическому алгоритму транспортными потоками на двух сообщающихся перекрестках. Опишем изучаемую систему на содержательном уровне. Входные потоки Π_1, Π_2 являются независимыми

стационарными и неординарными потоками без последействия. Требования потока Π_j, $j = 1, 2$, помещаются в накопитель O_j неограниченного объема; эти требования называются первичными. Обслуженные требования первого потока поступают в промежуточную очередь O_3, а из нее (после "проезда от перекрестка до перекрестка") — в очередь O_2 для дальнейшего обслуживания; эти требования называются вторичными и образуют входной поток Π_3. Обслуживающий прибор имеет n состояний $\Gamma^{(1)}, \Gamma^{(2)}, \ldots, \Gamma^{(n)}$. В состоянии $\Gamma^{(r)}$, $r = 1, 2, \ldots, n$, прибор проводит неслучайное время T_r и функционирует в одном из четырех режимов: 1) требования не обслуживаются, 2) обслуживается только требования из очереди O_1, 3) обслуживается только требования из очереди O_2, 4) обслуживаются требования из очередей O_1 и O_2. Смена состояний прибора происходит по циклическому алгоритму: после состояния $\Gamma^{(r)}$ осуществляется мгновенный переход в состояние $\Gamma^{(r\oplus 1)}$, где $r \oplus 1$ принимает значение $r + 1$ при $r < n$ и значение 1 при $r = n$. Процесс обслуживания удобно характеризовать не длительностями обслуживания произвольного требования, как принято в теории массового обслуживания, а потоками насыщения $\Pi_1^{\text{нас}}$, $\Pi_2^{\text{нас}}$ — выходными потоками системы обслуживания при максимально возможной загруженности ее накопителей и эксплуатации. Если обслуживающее устройство находится в состоянии $\Gamma^{(r)}$, при котором обслуживаются требования очереди O_j, то поток насыщения $\Pi_j^{\text{нас}}$ содержит $\ell_{r,j}$ требований. Отличительной особенностью данной системы является, во-первых, сложный поток первичных и вторичных требований, поступающий в очередь O_2; во-вторых, наличие задержки при перемещении требований из одной очередь на обслуживание в другую очередь на обслуживание — в теории сетей массового обслуживания предполагается, что перемещение требований между узлами сети осуществляется мгновенно.

Положим $\tau_0 = 0$ и пусть τ_i — последовательные моменты смены состояния обслуживающего устройства: $\tau_1 = T_1$, $\tau_2 = \tau_1 + T_2$, $\ldots$, $\tau_n = \tau_{n-1} + T_n$, $\tau_{n+1} = \tau_n + T_1$, $\ldots$. Будем рассматривать функционирование управляющей системы в дискретной временной шкале $\{\tau_i; i = 0,1,\ldots\}$. Определим схему, информацию, координаты и функцию этой управляющей системы. На схеме присутствуют следующие блоки: 1) внешняя среда, формирующая входные потоки; 2) входные потоки Π_1, Π_2, Π_3 требований — первый тип входных полюсов; 3) потоки насыщения $\Pi_1^{\text{нас}}$, $\Pi_2^{\text{нас}}$ второй тип входных полюсов; 4) накопители O_1, O_2, O_3 — внешняя память; 5) устройства по организации дисциплины очереди в накопителях — устройства переработки информации во внешней памяти; 6) обслуживающее устрой-

ство — внутренняя память; 7) граф смены состояний обслуживающего устройства — устройство переработки информации внутренней памяти; 8) выходные потоки $\Pi_1^{\text{вых}}$, $\Pi_2^{\text{вых}}$ — выходные полюса. Набор состояний среды, очередей в накопителях, обслуживающего устройства. потоков насыщения и потоков обслуженных требований полностью определяет информацию управляющей системы. Номера состояний случайной среды, входных потоков, накопителей, механизмов по формированию очереди и номер состояния обслуживающего устройства задают расположение блоков на схеме. Функция этой системы — обслуживание потоков по циклическому алгоритму.

Все объекты рассматриваются на некотором вероятностном пространстве $(\Omega, \mathcal{F}, \mathsf{P})$, где Ω — множество описаний ω элементарных исходов, $\mathcal{F}$ — σ-алгебра событий $A \subset \Omega$, P — вероятность на $\mathcal{F}$. Обозначим Γ^{I}, Γ^{II}, Γ^{III}, Γ^{IV} непустые множества состояний $\Gamma^{(r)}$, при которых реализуется первый, второй, третий и четвертый режимы функционирования прибора соответственно. Никакая пара $\Gamma^{(r)}$, $\Gamma^{(r\oplus 1)}$ не может принадлежать одному и тому же множеству из четырех. Пусть, далее, $\Gamma = \Gamma^{\mathrm{I}} \cup \Gamma^{\mathrm{II}} \cup \Gamma^{\mathrm{III}} \cup \Gamma^{\mathrm{IV}}$ — множество всех состояний прибора. Положим $X = \{0, 1, \ldots\} \times \{0, 1, \ldots\} \times \{0, 1, \ldots\}$. Введем отображение $u\colon \Gamma \to \Gamma$ равенством $u(\Gamma^{(r)}) = \Gamma^{(r\oplus 1)}$. Пусть Γ_i — состояние обслуживающего устройства в момент τ_i, $\kappa_{s,i}$ — число требований в очереди O_s в момент τ_i, $s = 1, 2, 3$, $\eta_{s,i}$ — число требований потока Π_s, поступивших за промежуток $(\tau_i, \tau_{i+1}]$, $\xi_{j,i}$ — число требований потока насыщения $\Pi_j^{\text{нас}}$ на промежутке $(\tau_i, \tau_{i+1}]$. Тогда имеют место следующие рекуррентные соотношения: $\Gamma_{i+1} = u(\Gamma_i)$, $\kappa_{1,i+1} = \max\{0, \kappa_{1,i} + \eta_{1,i} - \xi_{1,i}\}$, $\kappa_{2,i+1} = \max\{0, \kappa_{2,i} + \eta_{2,i} + \eta_{3,i} - \xi_{2,i}\}$, $\kappa_{3,i+1} = \max\{0, \kappa_{3,i} + \min\{\xi_{1,i}, \kappa_{1,i} + \eta_{1,i}\} - \eta_{3,i}\}$. Нелокальное описание входных потоков и потоков насыщения (см. [1]) производится перечислением свойств условных распределений маркированных точечных процессов $\{(\tau_i, \eta_{j,i}, \nu_i);\, i = 0, 1, \ldots\}$, $\{(\tau_i, \xi_{j,i}, \nu_i);\, i = 0, 1, \ldots\}$, $j = 1, 2$, $\{(\tau_i, \eta_{3,i}, \nu_i');\, i = 0, 1, \ldots\}$ с метками $\nu_i' = \Gamma_i$ и $\nu_i' = (\Gamma_i, \kappa_{3,i})$ требований на промежутке $(\tau_i, \tau_{i+1}]$. Будем считать, что условное распределение величины $\eta_{3,i}$ зависит только от ν_i' и случайная величина $\eta_{3,i}$ с положительными вероятностями принимает каждое из своих возможных значений $0, 1, \ldots, \kappa_{3,i}$.

Теорема 1. *Случайная последовательность*

$$\{(\Gamma_i, \kappa_{1,i}, \kappa_{2,i}, \kappa_{3,i});\, i = 0, 1, \ldots\} \tag{1}$$

при заданном начальном распределении вектора $(\Gamma_0, \kappa_{1,0}, \kappa_{2,0}, \kappa_{3,0})$ *является марковской цепью.*

Пусть $w = (w_1, w_2, w_3)$ — произвольный элемент из X. Введем множества $E_1' = \{(\Gamma^{(r)}, w)\colon \Gamma^{(r)} \in \Gamma^{\mathrm{II}} \cup \Gamma^{\mathrm{IV}}, w_1 > 0, w_3 < \ell_{r,1}\}$, $E_1 = \{(\gamma, w)\colon \gamma \in \Gamma^{\mathrm{I}} \cup \Gamma^{\mathrm{III}}, w \in X\}$, $E_2 = \{(\gamma, w)\colon \gamma \in \Gamma^{\mathrm{II}} \cup \Gamma^{\mathrm{IV}}, w_1 = 0\}$, $E_3 = \{(\Gamma^{(r)}, w)\colon \Gamma^{(r)} \in \Gamma^{\mathrm{II}} \cup \Gamma^{\mathrm{IV}}, w_1 > 0, w_3 \geq \ell_{r,1}\}$.

Теорема 2. *Множество состояний марковской цепи* (1) *есть объединение незамкнутого подмножества E_1' несущественных состояний и замкнутого подмножества $E_1 \cup E_2 \cup E_3$ существенных периодических состояний с периодом n.*

Список литературы

1. Федоткин М. А. Процессы обслуживания и управляющие системы // Математические проблемы кибернетики. Вып. 6. — М.: Наука, 1996. — С. 51–70.

2. Зорин А. В., Федоткин М. А. Оптимизация управления дважды стохастическими неординарными потоками в системах с разделением времени // Автоматика и телемеханика. — 2005. — № 7. — С. 102–111.

3. Ляпунов А. А., Яблонский С. В. Теоретические проблемы кибернетики // Проблемы кибернетики. — Вып. 9. — М.: Физматгиз, 1963. — С. 5–22.

УПРАВЛЕНИЕ ОДНОПРОЦЕССОРНЫМ ОБСЛУЖИВАНИЕМ ГРУППИРОВКИ СТАЦИОНАРНЫХ ОБЪЕКТОВ: МАТЕМАТИЧЕСКАЯ МОДЕЛЬ, АЛГОРИТМЫ, ВЫЧИСЛИТЕЛЬНАЯ СЛОЖНОСТЬ

Д. И. Коган (Москва),
Ю. С. Федосенко (Нижний Новгород)

1. Считается заданной группировка $O_n = \{\, o_1, o_2, \ldots, o_n \,\}$ стационарных объектов, расположенных в рабочей зоне Ξ обслуживающего процессора P. Зона Ξ представляет собой направленный отрезок L, начальная точка A которого является базовой для процессора; объекты пронумерованы в порядке возрастания их расстояний от точки A; конечная точка B отрезка L является местом расположения объекта o_n. Из точки A, начиная от момента времени $t = 0$, процессор поступательно перемещается к конечной точке B (прямой

рейс — λ_+), а затем, достигнув ее, также поступательно возвращается в точку A (обратный рейс — λ_-). При реализации цикла $\lambda_+\lambda_-$ процессор P выполняет однократное, без прерываний обслуживание объектов группировки O_n; обслуживание части объектов реализуется в рейсе λ_+, обслуживание оставшихся объектов — в рейсе λ_-. С каждым объектом o_j ассоциируется монотонно возрастающая (в нестрогом смысле) функция индивидуального штрафа $\varphi_j(t)$, выражающая зависящую от момента завершения его обслуживания величину потерь. В качестве примеров, адекватно описываемых рассматриваемой моделью, укажем технологии снабжения дизельным топливом судномзаправщиком плавучих технологических комплексов, осуществляющих русловую добычу нерудных материалов [1]. Близкие модели описывают процессы технического обслуживания магистральных линий электропередач, а также снабжения расходуемыми ресурсами орбитальных группировок спутников [2].

2. Пусть $l_1, l_2, \ldots, l_n$ — точки отрезка L, в которых расположены объекты $o_1, o_2, \ldots, o_n$ соответственно; точки l_n и B совпадают; $\gamma_{j-1,j}$ и $\gamma_{j,j-1}$ — нормы времени на перемещения процессора между точками l_{j-1} и l_j в рейсах λ_+ и λ_- соответственно, при этом $\gamma_{0,1}$ и $\gamma_{1,0}$ — нормы времени на перемещение процессора между точкой A и точкой l_1 в прямом и обратном рейсах; τ_j — продолжительность обслуживания процессором объекта o_j ($j = \overline{1,n}$). Все величины $\gamma_{j-1,j}$, $\gamma_{j,j-1}$, τ_j считаем целочисленными.

Стратегией обслуживания именуем произвольное подмножество элементов V из совокупности индексов $N = \{1, 2, \ldots, n\}$. Объекты o_j, где $j \in V$, в реализации стратегии V обслуживаются процессором в рейсе λ_+, все остальные объекты группы O_n — в рейсе λ_-. Для определенности полагаем, что объект o_n обслуживается при завершении процессором рейса λ_+, и, таким образом, $n \in V$. Обслуживание любого объекта o_j ($j \in N$), начинается от момента прибытия процессора в точку l_j при реализации определяемого стратегией V рейса; по завершению обслуживания процессор продолжает выполняемый рейс. Не связанные с обслуживанием объектов промежуточные простои процессора запрещены. Любая стратегия однозначно определяет моменты начала и завершения обслуживания каждого из объектов.

3. Задача 1 состоит в отыскании стратегии обслуживания, минимизирующей величину суммарного по всем объектам штрафа.

Алгоритм решения задачи 1 основан на принципе динамического программирования, оценка его вычислительной сложности псевдополиномиальна.

С точки зрения приложений важны следующие конкретизации за-

дачи 1 для $j = \overline{1,n}$: а) продолжительности обслуживания одинаковы ($\tau_j = \tau$); б) функции штрафа линейны ($\varphi_j(t) = a_j t + b_j$); в) функции штрафа являются простейшими кусочно-линейными ($\varphi_j(t) = 0$ при $t \in [0, d_j]$, $\varphi_j(t) = G_j(t - d_j)$ при $t > d_j$, G_j и d_j — неотрицательные константы); г) функции штрафа являются простейшими ступенчатыми ($\varphi_j(t) = 0$ при $t \in [0, d_j]$, $\varphi_j(t) = G_j$ при $t > d_j$).

Для случаев а) и б) имеются полиномиальные по верхней оценке числа элементарных операций решающие алгоритмы. Вычислительная сложность алгоритмов решения задачи 1 в случаях в) и г) определяется нижеследующими теоремами.

Теорема 1. *Задача* 1, *в которой все функции индивидуального штрафа являются простейшими кусочно-линейными, NP-трудна.*

Теорема 2. *Задача* 1, *в которой все функции индивидуального штрафа являются простейшими ступенчатыми, NP-трудна.*

4. Задача 2 порождается моделями обслуживания с директивными сроками (с каждым объектом o_j ассоциируется штраф $\varphi_j(t)$, равный нулю при $t \in [0, d_j]$ и определяемый монотонно возрастающей от нуля функцией $\Phi_j(t - d_j)$ при $t > d_j$ ($j = \overline{1,n}$)). В таких моделях произвольную стратегию V целесообразно оценивать двумя критериями: $K_1(V)$ — числом объектов, обслуживаемых с нарушениями директивных сроков и $K_2(V)$ — суммарным штрафом. Требуется отыскать стратегию, оптимальную по двум лексикографически упорядоченным [3] минимизируемым критериям $K_1(V)$, $K_2(V)$; при этом ведущим считается первый критерий. Алгоритм решения задачи 2 предусматривает её сведение к задаче 1; его вычислительная сложность определяется теоремой 3.

Теорема 3. *Задача* 2, *в которой функции индивидуального штрафа являются простейшими кусочно-линейными, NP-трудна.*

В доказательствах всех трёх теорем о труднорешаемости используется возможность полиномиального сведения NP-полной задачи Разбиение [4] к задачам, указанным в формулировках теорем 1–3.

5. Несмотря на полученные результаты об NP-трудности, выполненные по прикладным задачам расчеты потребовали вполне приемлемого расхода времени. Так, например, для каждой из реально возникших задач бункеровки топливом 18 20 технологических комплексов, ведущих добычу гравийной массы на трёхсоткилометровом русловом полигоне, синтез оптимального план-графика выполнялся ПК (процессор Celeron 1700 MHz, память 512 Mb) с расходом времени в пределах 7–10 минут; расчёты проводились в диспетчерской службе Камского грузового района в течение навигации ежедневно.

Список литературы

1. Коган Д. И., Федосенко А. Ю., Шлюгаев А. Ю. Задача одностадийного обслуживания добывающих комплексов в крупномасштабной акватории //Труды V Московской международной конференции по исследованию операций (М., 10-14 апр. 2007 г.) — М.: МАКС Пресс, 2007. — С. 60-62.

2. Shen H., Tsiotras P. Peer-to-peer refueling for circular satellite constellations// AIAA Journal of Guidance, Control, and Dynamics. — 2005. — V. 28, №. 6. — P. 1220–1230.

3. Подиновский В. В., Гаврилов В. М. Оптимизация по последовательно применяемым критериям. — М.: Сов. Радио, 1975.

4. Гэри М., Джонсон Д. Вычислительные машины и труднорешаемые задачи. — М.: Мир, 1982.

УСЛОВИЯ ПОЛИНОМИАЛЬНОСТИ ЧИСЛА ШАГОВ АЛГОРИТМОВ РАМ и РАСП ПРИ РЕАЛИЗАЦИИ ИХ НА МАШИНАХ ТЬЮРИНГА

Н. К. Косовский (Санкт-Петербург)

К началу XXI века большинство математиков, занимающихся оценками сложности вычислений у алгоритмов, предназначенных для использования на компьютерах, стали понимать важность изучения принадлежности классу **FP**, т. е. классу функций, вычислимых на машинах Тьюринга за полиномиальное число шагов относительно длины записи исходных данных. Более того, считается, что класс **FP** совпадает с классом эффективных вычислений (на основе обобщенного тезиса Черча (см., например, [4])).

Представление класса **FP** невозможно с помощью ограниченного произведения (П), которое может вывести за пределы этого класса. За его пределы не выводят суперпозиция и ограниченная словарная рекурсия совместно определяемых функций (совместная ограниченная словарная рекурсия).

Существенная трудность доказательства принадлежности алгоритма классу **FP** связана с тем, что многие численные алгоритмы используют косвенную адресацию при обработке массивов, для которой были созданы модели вычисления РАМ и РАСП — равнодоступная адресная машина (машина с произвольным доступом к

памяти) и она же с хранимой программой (машина с произвольным доступом к памяти и хранимой программой).

Ниже оценку числа шагов предлагается использовать в традиционном смысле, в частности, предложенном в [1]. Кроме того, можно использовать и БульРАСП (адресную машину с хранимой памятью, предложенную переводчиком книги [1] в конце раздела 1.4). То есть один шаг учитывается вне зависимости от длины записи операндов команды.

К сожалению, в этом случае при наличии операции умножения за полиномиальное число шагов на этих моделях можно вычислить функцию экспоненциального вида, например, x^y (при быстром вычислении), что невозможно сделать за полиномиальное число шагов на машине Тьюринга (длина записи результата задается экспонентой от длины записи y).

Ниже используется следующий критерий для оценки памяти: сумма длин всех наибольших абсолютных величин номеров и содержимых регистров, к которым было обращение.

Введем понятие дважды полиномиальной программы на основе приведенного определения времени и памяти работы программ, лишенное указанного недостатка, а также недостатка, отмеченного в [2], позволяющего за полиномиальное число шагов РАМ- и РАСП-программ решить NP-полную задачу ВЫПОЛНИМОСТЬ [4].

Речь идет о том, что экспоненциальная длина записи промежуточных результатов в РАМе и использование поразрядной конъюнкции для чисел в двоично представлении позволяет построить истинностную таблицу для любой пропозициональной формулы за число шагов, линейное от числа логических связок в этой формуле. Заключительный шаг состоит в проверке наличия значения 1 в столбце, являющемся результатом выполнения всех требуемых поразрядных логических операций над столбцами, задающими значения переменных (то есть над столбцами вида (1010...10), (1100...1100) и т. д., которые могут быть порождены за полином шагов от числа переменных). Таким образом, NP-полная задача ВЫПОЛНИМОСТЬ может быть решена за полином шагов работы РАМ-программы.

Действительно, поразрядная конъюнкция может быть выполнена подпрограммой на РАМе за линейное число шагов. Операция умножения (возведения в квадрат) — за n шагов позволяет вычислить 2^{2^n}.

РАМ-, БульРАСП- и РАСП-программу назовем дважды полиномиальной, если при любых исходных данных число ее шагов до остановки не превосходит полинома от длины записи исходных данных и сумма длин абсолютных величин содержимых всех регистров,

к которым было обращение, также не превосходит полинома от длины записи исходных данных.

Теорема. *Класс алгоритмов, реализованных дважды полиномиальными РАМ- и РАСП-программами с операцией умножения, а также БульРАСП-программами, совпадает с классом* ***FP****.*

Доказательство основывается на моделировании РАМ-, РАСП- и БульРАСП-программ машиной Тьюринга, полиномиальной по времени.

При этом массив регистров программ заменяется на оракульной ленте машины Тьюринга списком пар вида (номер регистра, содержимое регистра). А ограниченное полиномоми суммирование полиномов (Σ) является полиномом. Это применяется для получения верхней полиномиальной оценки времени и памяти при работе оракульной машины Тьюринга.

К числу важных преимуществ дважды полиномиальных программ по сравнению с машинами Тьюринга, работающими за полиномиальное число шагов, относится возможность в их терминах доказывать содержательные и достаточно адекватные верхние оценки сложности и для задач с небольшой (например, квадратичной) верхней оценкой числа шагов программ.

Заметим, что справедливость расширенного тезиса Черча для языка рефал-5 следует из работы [3], в которой для этого языка также было введено понятие объема изменений как произведение числа шагов рекурсивных обращений и максимальной длины записи промежуточных вычислений. Для понятия машины Тьюринга объем изменений ограничен сверху квадратом числа шагов.

В терминах объема изменений расширенный тезис Черча может быть может быть сформулирован следующим образом. *Класс эффективно вычислимых алгоритмов совпадает с классом алгоритмов рассматриваемого математического понятия алгоритма, при работе которых объем изменений ограничен сверху полиномом от длины записи исходных данных.*

Список литературы

1. Ахо А., Хопкрофт Дж., Ульман Дж. Построение и анализ вычислительных алгоритмов. — М.: Мир, 1979.

2. Косовский Н. К., Косовская Т. М. Полиномиальность и NP-трудность задачи вычисления знака постоянного терма // Математические вопросы кибернетики. Вып. 16. — 2007. — С. 125–128.

3. Косовский Н. К. Условия полиномиальности алгоритмов, реализуемых на машинах Тьюринга с оракулами-функциями // Материалы XVII Международной школы-семинара "Синтез и сложность управляющих систем" имени академика О. Б. Лупанова (Новосибирск, 27 октября–1 ноября 2008 г.). — Новосибирск: Изд-во Инсти-

тута математики, 2008. — С. 70–74.

4. Du D.-Z., Ko K.-I. Theory of computational complexity. — A Wiley-Interscience Publication. John Wiley & Sons, Inc, 2000.

О СЛОЖНОСТИ САМОКОРРЕКТИРУЮЩИХСЯ СХЕМ ДЛЯ СИММЕТРИЧЕСКИХ ПОРОГОВЫХ ФУНКЦИЙ

В. М. Краснов (Москва)

Будем рассматривать схемы из функциональных элементов в базисе $B = \{x\&\bar{y}, 1\}$ [1], построенные из надежных и ненадежных элементов. Каждый надежный элемент имеет вес p ($p > k+2$) и реализует некоторую приписанную ему функцию из B. Каждый ненадежный элемент в исправном состоянии реализует некоторую приписанную ему функцию из B, а в неисправном состоянии — константу δ ($\delta \in \{0, 1\}$). Вес каждого ненадежного элемента равен 1. Каждая функция из B может быть реализована как надежным, так и ненадежным элементами.

Схема в базисе B называется *k-самокорректирующейся относительно неисправностей типа δ*, если при переходе в неисправное состояние не более чем k произвольных ненадежных элементов она реализует ту же функцию, что и при исправном состоянии всех ее элементов (все неисправные элементы в схеме реализуют фиксированную константу δ) [2]. *Сложностью схемы* называется сумма весов всех элементов схемы, а *сложностью реализации булевой функции* — наименьшая из сложностей схем, реализующих эту функцию при исправном состоянии ненадежных элементов. Сложность схемы S обозначим через $L(S)$, а сложность реализации функции f схемами в базисе B, k-самокорректирующимися относительно неисправностей типа δ, — через $L^B_{k,\delta}(f)$. Если сложность k-самокорректирующейся относительно неисправностей типа δ схемы в базисе B, реализующей функцию f, равна $L^B_{k,\delta}(f)$, то такая схема называется *минимальной*.

Ниже рассматривается реализация монотонных симметрических булевых функций $f^n_2(x_1, ..., x_n) = \bigvee\limits_{1 \le i < j \le n} x_i x_j$ k-самокорректирующимися схемами.

Теорема. *При любом фиксированном* k *и* $p > k+2$

$$L_{k,\delta}(f_2^n) \sim (k+2)n.$$

Введем новый базис $B_1 = \{x\&\bar{y}, 1, 0, \bar{x}\}$, который помимо элементов базиса B содержит еще надежные элементы с нулевыми весами, реализующие булевы константы и инверсию. Схемы в базисе B_1 обладают следующими свойствами.

Свойство 1 [3]. *Если в* k*-самокорректирующейся схеме* S *на входы некоторых исправных двухвходовых элементов подаются константы, то эти элементы можно удалить и получить* k*-самокорректирующуюся схему, реализующую прежнюю функцию.*

Свойство 2. *Если в* k*-самокорректирующейся схеме* S *на оба входа какого-нибудь двухвходового элемента подается одна и та же функция* φ *или на один из входов подается* φ*, а на другой —* $\bar{\varphi}$*, то этот элемент можно удалить из* S *и получить* k*-самокорректирующуюся схему, реализующую прежнюю функцию.*

Можно считать, что в S с каждым входом схемы соединен, быть может, вход только одного и притом надежного инвертора и выход этого инвертора соединяется со входами только двухвходовых элементов(во всяком случае к такой минимальной сжеме можно, очевидно, исходную схему преобразовать путем удаления "лишних" инверторов и изменения соединений элементов).

Лемма. *При* $n \geq 3$ *справедливо неравенство*

$$L_k^B(f_2^n) \geq L_k^B(f_2^{n-1}) + 2 + k.$$

Доказательство. Докажем это утверждение сперва для базиса B_1. Для базиса B оно будет простым следствием. Пусть S — произвольная минимальная k-самокорректирующаяся схема, реализующая $f_2^n(\tilde{x})$, $n \geq 3$. Покажем, что из S можно удалить элементы с общим весом не менее $k+2$ и получить схему для f_2^{n-1} .

Введем в схеме S монотонную нумерацию вершин таким образом, чтобы для любой дуги номер начала дуги был меньше номера ее конца [4]. Выделим двухвходовой элемент E с минимальным номером. Из выбора E, минимальности схемы S и свойств 1, 2 следует, что на входы элемента E подаются (с отрицаниями или без отрицаний) различные переменные, скажем x_1 и x_2.

Пусть E надежный элемент. Подадим вместо x_1 константу 0. Получим схему, реализующую f_2^{n-1} от оставшихся переменных. При этом можно удалить элемент (по свойствам 1, 2) весом не менее $k+2$ (а именно E). Таким образом, в этом случае утверждение леммы выполняется.

Пусть E ненадежен. Если вход x_1 соединен со входом надежного элемента, то, как и выше, получим утверждение леммы.

Предположим, что имеется менее чем $k+2$ двухвходовых элементов, у каждого из которых хотя бы один из входов соединен со входом x_1 или с выходом надежного инвертора, реализующего $\bar{x}_1$. Рассмотрим случай, когда все они, кроме E вышли из строя. Подадим вместо x_2 такую константу, при которой на выходе элемента E реализуется константа. Полученная схема реализует функцию, не зависящую от x_1. Но $f_2^n(\widetilde{x})$ при $x_2 = 0$ зависит от x_1. Получили противоречие. Значит, рассматриваемых элементов в S не менее чем $k+2$ штук и эти элементы можно удалить из схемы при $x_1 \equiv 0$. Лемма доказана.

Доказательство теоремы. Нижняя оценка легко получается из утверждения леммы индукцией по n. В доказательсте верхней оценки используется модификация [4] конструкции Гринчука из [5].

Выражаю признательность Н. П. Редькину за постановку задачи и внимание к работе.

Работа выполнена при финансовой поддержке РФФИ (проект 08–01–00863), программы поддержки ведущих научных школ РФ (проект НШ–4437.2010.1) и программы фундаментальных исследований ОМН РАН «Алгебраические и комбинаторные методы математической кибернетики и информационные системы нового поколения».

Список литературы

1. Лупанов О. Б. Асимптотические оценки сложности управляющих систем. — М.: Изд-во МГУ, 1984.

2. Редькин Н. П. Надежность и диагностика схем. — М.: Изд-во МГУ, 1992.

3. Редькин Н. П. Асимптотически минимальные самокорректирующиеся схемы для одной последовательности булевых функций // Дискретный анализ и исследование операций. — 1996. — Т. 3, № 2. — С. 62–79.

4. Редькин Н. П. Дискретная математика. — М.: Физматлит, 2009.

5. Гринчук М. И. О монотонной сложности пороговых функций // Методы дискретного анализа в теории графов и сложности. Вып. 52. — Новосибирск: Институт математики СО РАН, 1992. — С. 41–48.

ОБ ИНВЕРСИОННОЙ СЛОЖНОСТИ САМОКОРРЕКТИРУЮЩИХСЯ СХЕМ ДЛЯ ОДНОЙ ПОСЛЕДОВАТЕЛЬНОСТИ БУЛЕВЫХ ФУНКЦИЙ

Т. И. Краснова (Москва)

Будем рассматривать схемы из надежных и ненадежных функциональных элементов в базисе $B = \{\&, -\}$ [1, 2]. Схема называется *k-самокорректирующейся*, если при переходе в неисправное состояние не более чем k произвольных ненадежных элементов она реализует ту же самую функцию, что и в исправном состоянии всех ее элементов [3]. Каждый надежный инвертор имеет вес p, где $p \geq k+1$, и всегда реализует инверсию. Каждый ненадежный инвертор имеет вес 1 и в исправном состоянии реализует инверсию, а в неисправном состоянии — булеву константу δ. Все конъюнкторы — надежные элементы (реализуют только конъюнцию) и имеют нулевой вес. Тогда $L_k^-(f)$ — наименьшая из сложностей k-самокорректирующихся схем, реализующих булеву функцию f; под *сложностью схем* понимается сумма весов всех элементов этой схемы.

Для монотонных симметрических пороговых булевых функций $f_2^n(x_1, ..., x_n) = \bigvee\limits_{1 \leq i < j \leq n} x_i x_j$ установлена асимптотика инверсионной сложности этих функций.

Теорема. *При любых фиксированных k и p, удовлетворяющих условию $p \geq k+1$,*

$$L_k^-(f_2^n) \sim (k+1)n.$$

Доказательство этой теоремы, как обычно, распадается на две части: получение нижней оценки $L_k^-(f_2^n) \gtrsim (k+1)n$ и получение верхней оценки $L_k^-(f_2^n) \lesssim (k+1)n$. Приведем вспомогательные утверждения, используемые при получении нижней оценки.

Вначале рассмотрим обычные (не обязательно самокорректирующиеся) схемы из функциональных элементов в базисе $B = \{\&, -\}$, реализующие булеву функцию $f(x_1, ..., x_m)$. Возьмем произвольную схему S в базисе B. Инвертор E^- назовем *x_i-блокиратором*, если E^- — единственный инвертор в каком-то пути [2] из входа "x_i" (отвечающего в схеме S переменной x_i) в E^-.

Лемма 1. *Если функция $f(x_1, ..., x_m)$, существенно зависящая от переменной x_i, не представима в виде*

$$f(x_1, ..., x_m) = x_i \& g(x_1, ..., x_m), \qquad (*)$$

а схема S реализует функцию f, то любой путь из входа "x_i" в выход схемы S содержит x_i-блокиратор.

С использованием леммы 1 доказывается.

Лемма 2. *Если k-самокорректирующаяся схема S реализует функцию $f(x_1, ..., x_m)$, существенно зависящую от переменной x_i и непредставимую в виде $(*)$, то общий вес x_i-блокираторов в S не меньше $k+1$.*

Заметим, что функция $f_2^n(\widetilde{x})$ существенно зависит от всех своих переменных и непредставима в виде (*). Нижние оценки для сложности реализации $f_2^n(\widetilde{x})$ k-самокорректирующимися схемами удобно доказывать в предположении, что на входы схем наряду с переменными подаются константы 0 и 1. Ясно, что получаемые оценки справедливы и для случая, когда на входы схем разрешается подавать только переменные. При этом предположении любая схема в рассматриваемом базисе обладает следующими свойствами [4].

Свойство 1. *Если в k-самокорректирующейся схеме S на выходе некоторого исправного элемента реализуется константа, то этот элемент можно удалить, получив k-самокорректирующуюся схему, реализующую ту же функцию, что и S.*

Свойство 2. *Если в k-самокорректирующейся схеме S хотя бы на один из входов некоторого исправного элемента подается константа, то этот элемент можно удалить, получив k-самокорректирующуюся схему, реализующую прежнюю функцию.*

Свойство 3. *Если в k-самокорректирующейся схеме S выход некоторого элемента E не является выходом схемы и не соединен с входами других элементов, то E можно удалить, получив k-самокорректирующуюся схему, которая реализует прежнюю функцию.*

С учетом этих свойств и леммы 2 устанавливается следующий определяющий для нижней оценки факт.

Лемма 3. *При $n \geq 3$, $p \geq k+1$ и любом натуральном k справедливо неравенство*

$$L_k^-(f_2^n) \geq L_k^-(f_2^{n-1}) + 1 + k.$$

Для доказательства верхней оценки используется конструкция Гринчука из [5].

Нижняя оценка теоремы легко получается из леммы 3 индукцией по n.

Для конъюнкторной сложности реализации функции $f_2^n(\widetilde{x})$ самокоррекктирующимися схемами в базисе B при $p \geq k+2$ установлена следующая асимптотика функции Шеннона:

$$L_k^{\&}(f_2^n) \sim (k+2)n.$$

Здесь предполагается, что каждый надежный конъюнктор имеет вес p, каждый ненадежный конъюнктор имеет вес 1, а все инверторы надежные элементы с нулевым весом.

Выражаю признательность Н. П. Редькину за постановку задачи и внимание к работе.

Работа выполнена при финансовой поддержке РФФИ (проект 08–01–00863), программы поддержки ведущих научных школ РФ (проект НШ–4437.2010.1) и программы фундаментальных исследований ОМН РАН «Алгебраические и комбинаторные методы математической кибернетики и информационные системы нового поколения».

Список литературы

1. Лупанов О. Б. Асимптотические оценки сложности управляющих систем. — М.: Изд-во МГУ, 1984.

2. Редькин Н. П. Дискретная математика. – М.: Физматлит. 2009.

3. Редькин Н. П. Надежность и диагностика схем. — М.: Изд-во МГУ, 1992.

4. Редькин Н. П. Асимптотически минимальные самокорректирующиеся схемы для одной последовательности булевых функций // Дискретный анализ и исследование операций. — 1996. — Т. 3, № 2. — С. 62–79.

5. Гринчук М. И. О монотонной сложности пороговых функций // Методы дискретного анализа в теории графов и сложности. Вып. 52. — Новосибирск: Институт математики СО РАН, 1992. — С. 41–48.

НЕКОТОРЫЕ ОЦЕНКИ СЛОЖНОСТИ ОРИЕНТИРОВАННЫХ КОНТАКТНЫХ СХЕМ С ОГРАНИЧЕННОЙ ПОЛУСТЕПЕНЬЮ ИСХОДА

С. А. Ложкин, А. Е. Шиганов (Москва)

В настоящей работе приводятся асимптотические оценки для сложности реализации булевых функций в одном классе ориентированных контактных схем (ОКС).

Обозначим через U_λ класс ОКС Σ таких, что полустепени исхода вершин Σ не превосходят λ. Сложностью $L(\Sigma)$ ОКС Σ называется число контактов в Σ. Сложностью $L_\lambda(f)$ булевой функции f называется минимальная сложность схемы Σ из класса U_λ, реализующей f. Определим функцию Шеннона

$$L_\lambda(n) = \max_{f(x_1,\ldots,x_n)} L_\lambda(f).$$

Из следующей теоремы вытекает нижняя оценка функции Шеннона $L_\lambda(n)$.

Теорема 1. *Пусть $\lambda \geqslant 2$. Для почти всех булевых функций f от n переменных выполнено неравенство*

$$L_\lambda(f) \geqslant \frac{\lambda}{\lambda-1} \cdot \frac{2^n}{n} \left(1 + \frac{-\frac{1}{\lambda-1}\log n - O(1)}{n}\right). \qquad (1)$$

Теорема 1 доказывается с использованием мощностных соображений (см., например, [1]).

Из работы [2] вытекает верхняя оценка функции Шеннона $L_\lambda(n)$ при $\lambda \geqslant 2$:

$$L_\lambda(n) \leqslant \frac{\lambda}{\lambda-1} \cdot \frac{2^n}{n} \left(1 + \frac{\frac{\lambda-2}{\lambda-1}\log n + O(1)}{n}\right). \qquad (2)$$

Отметим, что относительная погрешность (ОП) оценок (1), (2), т. е. отношение разности между верхней и нижней оценками функции Шеннона к ней самой, составляет $\frac{\log n + O(1)}{n}$.

Основной результат настоящей работы представлен в следующей теореме.

Теорема 2. *Пусть $\lambda \geqslant 2$, тогда выполнено неравенство*

$$L_\lambda(n) \leqslant \frac{\lambda}{\lambda-1} \cdot \frac{2^n}{n} \left(1 + \frac{-\frac{1}{\lambda-1}\log n + \log\log n + O(1)}{n}\right). \qquad (3)$$

Полученные оценки (1), (3) функции Шеннона $L_\lambda(n)$ имеют ОП вида $\frac{\log\log n + O(1)}{n}$.

Работа выполнена при финансовой поддержке РФФИ, грант 09-01-00817-а.

Список литературы

1. Ложкин С. А. Основы кибернетики. — М.: Изд-во МГУ, 2004.

2. Шиганов А. Е. О сложности ориентированных контактных схем с ограниченной полустепенью исхода // Учен. зап. Казан. ун-та. Сер. Физ.-матем. науки. — 2009. — Т. 151, кн. 2. — С. 164–172.

НЕОБХОДИМЫЕ УСЛОВИЯ ОПТИМАЛЬНОСТИ ВТОРОГО ПОРЯДКА ДЛЯ ДИСКРЕТНЫХ СИСТЕМ С НЕЛОКАЛЬНЫМИ УСЛОВИЯМИ

Г. Ю. Мехтиева, Я. А. Шарифов (Баку)

Рассмотрим задачу о минимуме функционала

$$J(u) = \varphi\left(x\left(t_0\right), x\left(t_1\right)\right) \tag{1}$$

при ограничениях

$$x\left(t+1\right) = f\left(t, x(t), u(t)\right), \quad t \in T = \left\{t_0, t_0+1, ..., t_1-1\right\}, \tag{2}$$

$$x(t_0) + Bx\left(t_1\right) = C, \tag{3}$$

$$u(t) \in V \subset R^r, \quad t \in T. \tag{4}$$

Здесь $x(t)$ — n-мерный вектор фазовых переменных, $u\left(t\right)$ — r-мерный вектор управляющих воздействий со значениями из заданного непустого, ограниченного и открытого множества V; $\varphi(x, y)$ — дважды непрерывно дифференцируемая скалярная функция; t_0, t_1 — заданы, $C \in R^{n\times 1}, B \in R^{n\times n}$ — заданная матрица, причем, $\|B\| < 1$; $f\left(t, x(t), u(t)\right)$ — заданная n-мерная вектор-функция, непрерывная по совокупности переменных вместе с частными производными по (x, u) до второго порядка включительно.

Введем функцию Понтрягина: $H\left(t, x, u, \psi\right) =< \psi, f(t, x, u) >$, где $\psi(t)$ является решением следующей краевой задачи

$$\psi(t-1) = H_x\left(t, x(t), u(t), \psi(t)\right), \tag{5}$$

$$\psi(t_1-1)+B'\psi(t_0-1) = B'\varphi_{x(t_0)}\left(x(t_0), x(t_1)\right)-\varphi_{x(t_1)}\left(x(t_0), x(t_1)\right). \tag{6}$$

В случае открытости области управления V для оптимальности допустимого управления $u(t)$ необходимо, чтобы вдоль оптимального процесса $(u(t), x(t))$ выполнялось следующее соотношение:

$$H_u\left(\theta, x(\theta), u(\theta), \psi(\theta)\right) = 0 \quad \forall\theta \in T. \tag{7}$$

Соотношение (7) называется аналогом управления Эйлера для задачи (1)–(4) и является необходимым условием оптимальности первого порядка.

Допустимое управление $u(t)$, удовлетворяющее соотношению (7) называется *классической экстремалью* в задаче (1)–(4).

Для оптимальности классической экстремали в задаче (1)–(4) необходимо, чтобы вдоль процесса $(u(t), x(t))$ вторая вариация функционала $J(u)$ для любой допустимой вариации управления была неотрицательна, т. е. неравенство

$$\delta x'(t_0)\,\varphi_{x(t_0)x(t_0)}(x(t_0), x(t_1))\,\delta x(t_0) + 2\delta x'(t_1)\varphi_{x(t_0)x(t_1)}(x(t_0), x(t_1)) \times$$

$$\times \delta x(t_0) + \delta x'(t_1)\varphi_{x(t_1)x(t_1)}(x(t_0), x(t_1))\,\delta x(t_1) - \sum_{t=t_0}^{t_1-1} [\delta x'(t) H_{xx}(t)\delta x(t_1) +$$

$$+ 2\delta u'(t) H_{xx}(t)\delta x(t) + \delta u'(x) H_{uu}(t)\delta u(t)] \geq 0 \qquad (8)$$

выполнялось для любого $\delta u(t) \in R^r$, где $\delta x(t)$ является решением следующей краевой задачи:

$$\delta x(t+1) = f_x(t)\delta x(t) + f_u(t)\delta u(t), \quad t \in T \qquad (9)$$

$$\delta x(t_0) + B\delta x(t_1) = 0. \qquad (10)$$

Согласно [1], любое решение уравнения (9) можно представить в виде:

$$\delta x(t) = \Phi(t, t_0 - 1)\,\delta x(t_0) + \sum_{\tau=t_0}^{t_1-1} \Phi(t, \tau) f_u(\tau)\delta u(\tau), \qquad (11)$$

где матричная функция $\Phi(t, t-1)$ является решением следующей системы:

$$\Phi(t, \tau - 1) = \Phi(t, \tau) - f_x(\tau), \qquad (12)$$

$$\Phi(t, t-1) = E, \qquad (13)$$

где E — единичная матрица размерности $n \times n$. Можно показать, что решение краевой задачи (9), (10) можно представить в виде:

$$\delta x(t) = -\Phi(t, t_0 - 1)\,[E + B\Phi(t_1, t_0 - 1)]^{-1} \times$$

$$\times \sum_{\tau=t_0}^{t_1-1} \Phi(t, \tau) f_u(\tau)\delta u(\tau) + \sum_{\tau=t_0}^{t-1} \Phi(t, \tau) f_u(\tau)\delta u(\tau).$$

Введем матрицу-функцию

$$R(\tau, s) = -\Phi'(t_1, \tau) L'(t_0, t_1)\,\varphi_{xx} L(t_0, t_1)\,\Phi(t_1, s) -$$

$$-\Phi'(t_1, \tau) L'(t_0, t_1)\,(E - \Phi(t_1, t_0 - 1))' \times$$

$$\times\varphi_{yy}\left(E-\Phi\left(t_1,t_0-1\right)\right)L\left(t_0,t_1\right)\Phi(t_1,s)-$$

$$-2\Phi'(t,\tau)L'\left(t_0,t_1\right)\left(E-\Phi\left(t_1,t_0-1\right)\right)'\varphi_{xy}L\left(t_0,t_1\right)\Phi(t,s)+$$

$$+\sum_{t=\max(\tau,s)+1}^{t_1-1}\Phi'(\tau,t)\frac{\partial^2 H}{\partial x^2}\Phi(t,s)-\Phi'(t_1,\tau)L'\left(t_0,t_1\right)\Phi'\left(t,t_0-1\right)\times$$

$$\times\frac{\partial^2 H}{\partial x^2}\Phi(t,s)-\Phi'(t,\tau)\frac{\partial^2 H}{\partial x^2}\Phi(t,t_0-1)L\left(t_0,t_1\right)\Phi'(t_1,s)+$$

$$+\Phi'(t_1,\tau)L'\left(t_0,t_1\right)\Phi'\left(t,t_0-1\right)\frac{\partial^2 H}{\partial x^2}\Phi(t,t_0-1)L\left(t_0,t_1\right)\Phi(t_1,s),$$

где $L\left(t_0,t_1\right)=\left(E+B\Phi\left(t_1,t_0-1\right)\right)^{-1}$.

Тогда соотношение (8) можно переписать в виде

$$\sum_{\tau=t_0}^{t_1-1}\sum_{s=t_0}^{t_1-1}\delta u'(\tau)f_u'(\tau)R(\tau,s)f_u(s)\delta u(s)+$$

$$+2\sum_{t=t_0}^{t_1-1}\left[\sum_{s=t_0}^{t_1-1}\delta u'(t)H_{ux}\left[\Phi(t,t_0-1)L\left(t_0,t_1\right)\sum_{s=t_0}^{t_1-1}\Phi(t_1,s)f_u(s)\right]\delta u(s)+\right.$$

$$\left.+\sum_{s=t_0}^{t-1}\delta u'(t)H_{ux}\Phi(t,s)f_u(s)\right]\delta u(s)+\sum_{t=t_0}^{t_1-1}\delta u'(t)H_{uu}(t)\delta u(t)\le 0. \quad (15)$$

Таким образом, доказана

Теорема. *Для оптимальности классической экстремали в рассматриваемой задаче необходимо, чтобы неравенство* (15) *выполнялось для любого* $\delta u(t)\in R^r, t\in T$.

Отметим, что при $B=0$ из (15) получается результаты [1, стр. 107].

Список литературы

1. Мансимов К. Б. Дискретные системы — Баку: Изд-во БГУ, 2002.

О РАНГЕ НЕЯВНЫХ ПРЕДСТАВЛЕНИЙ НАД ОДНИМ КЛАССОМ ФУНКЦИЙ ТРЕХЗНАЧНОЙ ЛОГИКИ

Е. В. Михайлец (Москва)

Рассмотрим систему функций k-значной логики A, $A \subseteq P_k$. *Системой неявных уравнений* над системой функций A будем называть всякую систему уравнений вида

$$\begin{cases} \Phi_1(x_1, \ldots, x_n, y) = \Psi_1(x_1, \ldots, x_n, y), \\ \ldots \\ \Phi_q(x_1, \ldots, x_n, y) = \Psi_q(x_1, \ldots, x_n, y), \end{cases}$$

где левые и правые части уравнений представляют собой суперпозиции над системой функций A или тривиальные функции, т. е. $\Phi_i, \Psi_i \in [A \cup \{x\}]$, $1 \leq i \leq q$.

Будем говорить, что функция $f(x_1, \ldots, x_n)$ k-значной логики *неявно выразима* над системой функций A, если существует система неявных уравнений над A указанного вида, имеющая при любых фиксированных значениях $x_1, \ldots, x_n$ единственное решение $y = f(x_1, \ldots, x_n)$. При этом соответствующую систему уравнений будем называть *неявным представлением* функции $f(x_1, \ldots, x_n)$ над A.

Множество всех функций f, $f \in P_k$, неявно выразимых над системой функций A, назовем *неявным расширением* системы A и будем обозначать через $I(A)$ [1].

Если неявное расширение системы A содержит все функции k-значной логики, т. е. $I(A) = P_k$, то систему функций A называют *неявно полной* в P_k.

Рассмотрим произвольную функцию f из неявного расширения некоторой системы A функций k-значной логики, $f \in I(A)$. Следуя [1], назовем *рангом* функции f над системой A и будем обозначать через $m_A(f)$ наименьшее число уравнений, достаточное для построения неявного представления f над A.

Далее, введем функцию Шеннона $m_A(n) = \max m_A(f)$, называемую *ранговой функцией* системы A (максимум берется по всем функциям k-значной логики, принадлежащим неявному расширению системы A и существенно зависящим не более чем от n переменных).

Изначально понятие неявной выразимости функций k-значной логики было введено А. В. Кузнецовым [2]. В дальнейшем исследования в этой области были продолжены в работах О. М. Касим-Заде, который, в частности, решил проблему неявной выразимости и неявной полноты в P_2 и получил для всех систем булевых функций

либо точное выражение, либо порядок роста ранговой функции [1]. Из результатов работы [1], в частности, следует, что для любой неявно полной системы функций в P_2 ранговая функция имеет либо константный, либо линейный по n порядок роста.

В P_3 проблема неявной полноты решена Е. А. Ореховой. В ее работе [4] описаны двадцать семь минимальных неявно полных замкнутых по суперпозиции классов функций в P_3 и доказано, что произвольная система функций трехзначной логики неявно полна тогда и только тогда, когда ее замыкание по суперпозиции содержит хотя бы один из данных минимальных неявно полных классов.

Перед автором стояла задача исследовать поведение ранговых функций для всех двадцати семи минимальных неявно полных классов в P_3, описанных Е. А. Ореховой в [4].

С точностью до двойственности эти двадцать семь классов функций делятся на шесть классов эквивалентности. Каждый класс эквивалентности содержит двойственные друг другу классы функций. Так как ранговые функции двойственных систем функций совпадают, достаточно рассмотреть шесть минимальных неявно полных замкнутых классов, по одному представителю из каждого класса эквивалентности.

Автором было изучено поведение ранговой функции для всех шести классов в P_3. Для двух из них были получены экспоненциальные нижние и верхние оценки ранговой функции [3], для оставшихся четырех классов порядок роста ранговой функции оказался линейным.

Сформулируем результаты, касающиеся упомянутых линейных оценок роста ранговой функции. Для задания функций одной и двух переменных в P_3 будем использовать таблицы значений [4].

Обозначим через W_1, W_2, W_3, W_4 замыкания по суперпозиции следующих систем функций соответственно:

0	0	0	0	2	2	0	2
0	0	0	2	2	2	0	2
0	0	2	2	2	2	0	2

,

0	0	0	0	1	1	0	1
0	1	1	1	1	1	0	1
0	1	1	1	1	1	1	1

,

0	0	2	0	1	2	2	
0	1	2	1	1	2	2	
0	0	2	0	0	2	1	

,

0	0	2	0	1	2	0	0	0	1
0	1	2	1	1	2	0	0	2	1
2	2	2	2	2	2	0	0	2	1

.

Теорема. *Если система функций A совпадает с одним из классов W_1, W_2, W_3, то при всех натуральных n справедливо равенство*

$$m_A(n) = n + 2.$$

Если система A совпадает с W_4, то при всех натуральных n выполняются соотношения

$$\left\lceil \frac{n}{2} \right\rceil + 1 \leq m_A(n) \leq \left\lceil \frac{3n}{2} \right\rceil + 2.$$

Автор выражает благодарность своему научному руководителю О. М. Касим-Заде за всестороннее внимание к данной работе.

Работа выполнена при финансовой поддержке РФФИ (проект 08–01–00863), программы "Ведущие научные школы РФ" (проект НШ–4437.2010.1) и программы фундаментальных исследований Отделения математических наук РАН "Алгебраические и комбинаторные методы математической кибернетики и информационные системы нового поколения".

Список литературы

1. Касим-Заде О. М. Об одной метрической характеристике неявных и параметрических представлений булевых функций // Математические вопросы кибернетики. Вып. 6. — М.: Наука. Физматлит, 1996. — С. 133–188.

2. Кузнецов А. В. О средствах для обнаружения невыводимости или невыразимости // Логический вывод. — М.: Наука, 1979. — С. 5–33.

3. Михайлец Е. В. О ранге неявных представлений над одним классом функций трехзначной логики // Материалы VII Молодежной научной школы по дискретной математике и ее приложениям (Москва, ИПМ им. М. В. Келдыша РАН, 2009). — М.: Изд-во ИПМ, 2009.

4. Орехова Е. А. Об одном критерии неявной полноты в трехзначной логике // Математические вопросы кибернетики. Вып. 12. — М.: Наука. Физматлит, 2003. — С. 27–74.

ОЦЕНКИ СЛОЖНОСТИ ВЫЧИСЛЕНИЯ ХАРАКТЕРИСТИЧЕСКИХ ФУНКЦИЙ БЧХ-КОДОВ ВЕТВЯЩИМИСЯ ПРОГРАММАМИ

Е. А. Окольнишникова (Новосибирск)

Пусть B_{2r+1} — последовательность характеристических функций БЧХ–кодов с параметрами (n, M_n, d_n), где $d \geq 2r+1$, $M \geq$

$2^n/(n+1)^r$, где n — число переменных, M — число кодовых вершин, d_n — минимальное расстояние между двумя кодовыми вершинами.

Рассматривается вычисление характеристических функций БЧХ-кодов недетерминированными ветвящимися программами. В [1] для широкого спектра параметров БЧХ-кодов были получены нижние оценки сложности вычисления характеристических функций этих кодов детерминированными программами. При этом была получена нижняя оценка $\Omega(n \log n/ \log\log n)$ для сложности вычисления таких функций при некоторых значениях параметров БЧХ-кодов.

В [1, 2] была сформулирована теорема (теорема о сведении), которая позволяет сводить получение нижних оценок сложности вычисления функций ветвящимися программами (детерминированными [1] и недетерминированными [1, 2]) ветвящимися программами без ограничений к получению нижних оценок сложности подфункций рассматриваемой функции ветвящимися программами с ограничениями (k-программами).

В [3] была показано, что существуют параметры БЧХ-кодов, для которых нижняя оценка сложности характеристических функций этих кодов равна $\Omega(n \log n)$. Оценка была получена использованием теоремы о сведении [2] и результатов по нижним оценкам сложности ветвящихся k-программам из [4, 5].

Используя теорему о сведении и результаты [1, 2, 4, 5] можно доказать теорему о нижних оценках сложности для широкого спектра параметров БЧХ-кодов.

Теорема. *Пусть* $\{B_{2r+1}\}$ *— последовательность характеристических функций БЧХ–кодов с параметрами* (n, M_n, d_n), *где* $d \geq 2r+1$, $M \geq 2^n/(n+1)^r$. *Если* $r_n \to \infty$ *и* $n/r_n^2 \to \infty$ *при* $n \to \infty$, *то справедливы неравенства*

$$\mathrm{NBP}(B_{2r+1}) \succeq \begin{cases} r, & \text{если } r \preceq \ln n/\ln\ln n; \\ \ln n/\ln\ln n, & \text{если } \ln n/\ln\ln n \preceq r \\ & \qquad \text{и } r \preceq \log n/\log\log n; \\ \ln n, & \text{если } \log n/\log\log n \preceq r \preceq n^{C_0}, \\ & \quad \text{где } 0 < C_0 < 1/2 \text{ — константа}; \\ \ln n/r^2, & \text{если } \log r/\log n \to 1/2 \text{ при } n \to \infty. \end{cases}$$

Теорема. *Для характеристической функции БЧХ–кода* B_{2r+1} *справедливы оценки*

$$\mathrm{NBP}(B_{2r+1}) \preceq r\, n \ln n.$$

Работа выполнена при финансовой поддержке РФФИ, проект 09-01-00528-а.

Список литературы

1. Окольнишникова Е. А. Нижние оценки сложности реализации характеристических функций двоичных кодов бинарными программами // Методы дискретного анализа в синтезе реализаций булевых функций: Сб. науч. тр. Вып. 51. — Новосибирск: Ин-т математики СО АН СССР, 1991. — С. 61–83.

2. Окольнишникова Е. А. Об одном методе получения нижних оценок сложности реализации булевых функций недетерминированными ветвящимися программами // Дискрет. анализ и исслед. операций. Сер. 1. — 2001. — Т. 8, № 4. — С. 76–112.

3. Окольнишникова Е. А. Нижняя оценка сложности вычисления характеристических функций БЧХ-кодов ветвящимися программами // Дискрет. анализ и исслед. операций. — 2009. — Т. 16, № 5. — С. 69–77.

4. Borodin A., Razborov A., Smolensky R. On lower bounds for read-k-times branching programs // Computational Complexity. — 1993. — V. 3, № 1. — P. 1–18.

5. Thathachar J. S. On separating the read-k-times program hierarchy // Proc. of the 30th Ann. ACM Symp. on Theory of Computing, STOC'98 (Dallas, May 23–26, 1998). — New York: ACM, 1999. — P. 653–662.

О СЛОЖНОСТИ САМОКОРРЕКТИРУЮЩИХСЯ КОНТАКТНЫХ СХЕМ ДЛЯ БУЛЕВЫХ ФУНКЦИЙ С МАЛЫМ ЧИСЛОМ ЕДИНИЦ

Н. П. Редькин (Москва)

Будем рассматривать контактные схемы [1]. Пусть схема S реализует булеву функцию $f(\widetilde{x})$, $\widetilde{x} = (x_1, \ldots, x_n)$, и под воздействием источника неисправностей [2, 3] в S возможны обрывы и замыкания контактов [3, 4]. В случае *обрыва* контакт (рассматриваемый как двухполюсная контактная схема) реализует константу 0, а в случае *замыкания* — константу 1. Схема S *корректирует* a *обрывов и* b *замыканий*, т. е. является (a, b)-самокорректирующейся, если в случае обрывов не более чем a контактов и замыканий не более

чем b контактов эта схема реализует ту же функцию, что и в исправном состоянии.

Обозначим через $L(S)$ *сложность* контактной схемы S, т. е. число контактов в ней. Пусть $L_{a,b}(f) = \min L(S)$, где минимум берётся по всем (a,b)-самокорректирующимся контактным схемам, реализующим булеву функцию f; *функция Шеннона* $L_{a,b}(f)$ задаёт *сложность реализации* булевой функции f. Ниже нас будет интересовать сложность реализации (a,b)-самокорректирующимися контактными схемами булевых функций с малым числом единиц из класса $F_{n,k}$, состоящего из всех тех булевых функций от n переменных, каждая из которых обращается в единицу ровно на k наборах значений переменных, а k мало сравнительно с n.

Близкие к окончательным результаты о сложности реализации функций из $F_{n,k}$ обычными (несамокорректирующимися) параллельно-последовательными контактными схемами получил Б. И. Фиников [5] в случае, когда k меньше $\log_2 n$. В [6] введены понятия сильных и слабых переменных булевых функций и с использованием этих понятий получены новые нижние оценки, позволившие получить асимптотики для сложности реализации булевых функций с малым числом единиц схемами из функциональных элементов. Эти понятия и представленные в [6] конструкции позволяют получить асимптотики и для сложности реализации функции из $F_{n,k}$ (a,b)-самокорректирующимися контактными схемами.

Пусть $f(x_1, \ldots, x_n)$ — произвольная булева функция из $F_{n,k}$, обращающаяся в единицу на наборах $\widetilde{\sigma}_1, \ldots, \widetilde{\sigma}_k$, где $\widetilde{\sigma}_i = (\sigma_{i,1}, \ldots, \sigma_{i,n})$, $i = 1, \ldots, k$. Функции f сопоставим $k \times n$ матрицу M_f, строками которой являются наборы $\widetilde{\sigma}_1, \ldots, \widetilde{\sigma}_k$, а j-й столбец данной матрицы отвечает переменной x_j, $j = 1, \ldots, n$. Столбцы матрицы M_f разобьём на группы одинаковых между собой столбцов. Для произвольного набора $\widetilde{\tau}$ длины (или, точнее, высоты) k через $M_{\widetilde{\tau}}$ обозначим группу столбцов (или подматрицу матрицы M_f, составленную из столбцов), равных $\widetilde{\tau}$; для каких-то $\widetilde{\tau}$ группы $M_{\widetilde{\tau}}$ могут оказаться пустыми. Непустую группу столбцов $M_{\widetilde{\tau}}$ будем считать *сильной*, если она содержит не менее двух столбцов $\widetilde{\tau}$ и в этих столбцах имеются как нули, так и единицы; переменные отвечающие столбцам из сильной группы, также будем считать *сильными*. Все остальные непустые группы и переменные, не относящиеся к сильным, будем считать *слабыми*.

Теорема. *Пусть a, b — произвольная пара неотрицательных целых чисел, а c — какая-нибудь бóльшая единицы константа. Пусть, далее, у булевой функции $f(x_1, \ldots, x_n)$ из класса F_{n,k_n} име-*

ется m_n сильных переменных, а параметр k_n удовлетворяет условию

$$1 \le k_n \le \log_2 n - c \log_2 \log_2 n.$$

Тогда

$$L_{a,b}(f) \sim (a+1)(b+1)(n+m_n).$$

При конструктивном доказательстве верхней оценки $L_{a,b}(f) \lesssim (a+1)(b+1)(n+m_n)$ используется фактически та же модификация метода Финикова, которая применялась автором в [6] при реализации булевых функций из F_{n,k_n} схемами из функциональных элементов в базисе $\{\&, \vee, -\}$. Нижняя оценка $L_{a,b}(f) \ge (a+1)(b+1)(n+m_n)$ получается с использованием свойств булевых функций, определяемых наличием сильных переменных, и способа оценки сложности сетей из работы Мура и Шеннона [7].

В заключение отметим тот заслуживающий внимания факт, что утверждение теоремы распространяется на *все* булевы функции из F_{n,k_n}.

Работа выполнена при финансовой поддержке РФФИ (проект 08–01–00863) и программы государственной поддержки ведущих научных школ РФ (проект НШ–4437.2010.1).

Список литературы

1. Лупанов О. Б. Асимптотические оценки сложности управляющих систем. — М.: Изд-во МГУ, 1984.

2. Яблонский С. В. Элементы математической кибернетики. — М.: Высшая школа, 2007.

3. Яблонский С. В. Некоторые вопросы надёжности и контроля управляющих схем // Математические вопросы кибернетики. Вып. 1. — М.: Наука. Физматлит, 1988.

4. Редькин Н. П. Надёжность и диагностика схем. — М.: Изд-во МГУ, 1992.

5. Фиников Б. И. Об одном семействе классов функций алгебры логики и их реализации в классе П-схем // Докл. АН СССР. — 1957. — Т. 115, № 2. — С. 247–248.

6. Редькин Н. П. О сложности булевых функций с малым числом единиц // Дискретная математика. — 2004. — Т. 3, № 4. — С. 20–31.

7. Moore E. F., Shannon C. E. Reliable circuits using less reliable relays // Journ. Franklin Institute. — 1956. — V. 262, № 3. — P. 191–208; № 4. — P. 281–297. [Русский перевод: Кибернетический сборник. Вып 1. — М.: ИЛ, 1960. — С. 109–148.]

ОБРАТНАЯ ЗАДАЧА ДЛЯ НЕЛИНЕЙНЫХ СИСТЕМ С НЕИЗВЕСТНЫМИ ПЕРЕМЕННЫМИ ПАРАМЕТРАМИ

Е. Я. Ройтенберг (Москва)

Пусть E банахово пространство и R нормированное кольцо линейных ограниченных операторов, отображающих E в себя. Рассмотрим дифференциальное уравнение

$$x' = A(t)x + \varphi(x,t) + p_1(t), \quad x(t_0) = x_0 \in S_p(\zeta_0). \tag{1}$$

Здесь $x(t)$ — неизвестное решение задачи (1), непрерывно дифференцируемая при $t \in \mathcal{T} = [t_0, \infty)$ вектор-функция со значениями из E; $A(t)$ — равномерно-ограниченная и непрерывная (в смысле нормы опреаторов) при $t \in \mathcal{T}$ оператор-функция со значениями из R; $\varphi(x,t)$ — нелинейный оператор, определенный на произведении $E \times \mathcal{T}$ со значениями из E, непрерывный по $t \in \mathcal{T}$ и удовлетворяющий для любых ζ и x из E условию $||\varphi(\zeta,t) - \varphi(x,t)|| \le q||\zeta - x||$; $p_1(t)$ — неизвестная, непрерывная при $t \in \mathcal{T}$ вектор-функция со значениями из E, такая, что $||p_1(t)|| \le k_1$, $t \in \mathcal{T}$; x_0 — постоянный вектор; $S_p(\zeta_0)$ — шар в E радиуса ρ с центром в точке ζ_0. Вектор x_0 неизвестен, но известна вектор-функция $y(t)$, $t \in \mathcal{T}$ со значениями из E:

$$y(t) = C(t)x(t) + p_2(t), \tag{2}$$

которую будем называть следом решения $x(t)$ задачи (1). Здесь $p_2(t)$ неизвестная, непрерывная при $t \in \mathcal{T}$ вектор-функция из E, такая, что $||p_2(t)|| \le k_2$, $t \in \mathcal{T}$, $C(t)$ — непрерывная при $t \in \mathcal{T}$ оператор-функция со значениями из R, $||C(t)|| \le c_1$, $t \in \mathcal{T}$, для которой не предполагается существования оператор-функции $C^{-1}(t)$, $t \in \mathcal{T}$.

Найдем дифференциальное уравнение, решение которого дает оценку решения задачи (1).

Рассмотрим вспомогательную задачу Коши

$$\zeta' = A(t)\zeta + \varphi(\zeta,t) + u(t), \quad \zeta(t_0) = \zeta_0, \tag{3}$$

решение которой предполагается известным. Здесь $\zeta(t)$ — непрерывно-дифференцируемая при $t \in \mathcal{T}$ вектор-функция со значениями из E; $u(t)$ — подлежащая определению вектор–функция, непрерывная для $t \in \mathcal{T}$ со значениями из E. След решения $\zeta(t)$ задачи (3) обозначим через $\eta(t)$, $t \in \mathcal{T}$,

$$\eta(t) = C(T)\zeta(t). \tag{4}$$

В пространстве E рассмотрим вектор–функцию

$$z = \zeta - x. \tag{5}$$

Тогда

$$z' = A(t)z + F(z,t) + u(t) - p_1(t), \quad z(t_0) = z_0, \tag{6}$$

где $||z_0|| \le \rho$, $\varphi(\zeta,t) - \varphi(x,t) = F(z,t)$, $||F(z,t)|| \le q||z||$. В качестве $u(t)$ берем вектор–функцию

$$u(t) = B(t)C(t)z(t), \tag{7}$$

где $B(t)$ — непрерывная при $t \in \mathcal{T}$ оператор-функция из R, такая, что $||B(t)|| \le b_1$, $t \in \mathcal{T}$.

Теорема. *Для нахождения дифференциального уравнения* (3), *решение которого дает оценку решения* $x(t)$ *задачи* (1), *достаточно так выбрать оператор* $B(t) = B_1(t) \subset R$, *чтобы существовали положительные числа* T, K, *для которых выполнены условия*
а) $||U(t_1)U^{-1}(t_2)|| \le K$ *при* $0 \le t_1 - t_2 \le T$;
б) для всяких $z \in E$ *и* $t \ge 0$ *имеется такое* $\theta_{z,t}$, $(0 \le \theta_{z,t} \le T)$, *что* $||U(t+\theta_{z,t})U^{-1}(t)z|| \le q_1||z(t)||$, *где* U — *решение операторного уравнения*

$$U' = \mathcal{A}(t)U, \quad U(t_0) = I.$$

Здесь $\mathcal{A}(t) = A(t) + B_1(t)C(t)$.

Для доказательства отметим, что при выполнении этих условий для решения уравнения

$$z' = \mathcal{A}(t)z + F(z,t) - p_1(t)$$

имеет место оценка

$$||z(t)|| \le N_0 e^{-\nu_0(t-t_0)}||z(t_0)|| + \frac{N_0\delta}{\nu}\left[1 - e^{-\nu(t-t_0)}\right],$$

где

$$\nu = \nu_0 - N_0 q, \quad \delta = \varkappa_1 + b_1\varkappa_2,$$
$$\varkappa_1 \ge k_1, \quad \varkappa_2 \ge k_2,$$
$$N_0 = \frac{K}{q_1}, \quad \nu_0 = \frac{1}{T}\ln\frac{1}{q_1} > 0.$$

Следствие. *Если предположить равномерную ограниченность решения* $x(t)$, $t \in \mathcal{T}$, *задачи* (1) *при* $p_1(t) \equiv 0$, $t \in \mathcal{T}$, *то теорема верна для случая, когда уравнение* (1) *имеет вид*

$$x' = (A(t) + \Xi(t))x + \varphi(x,t) + p_1(t),$$

где $\Xi(t)$, $t \in \mathcal{T}$, *неизвестная, непрерывная оператор-функция, такая, что* $||\Xi(t)|| \le k_3$, $t \in \mathcal{T}$, *а соотношение* (2) *имеет вид*

$$y(t) = [C(t) + \Phi(t)]x(t) + p_2(t),$$

где $\Phi(t)$, $t \in \mathcal{T}$, *неизвестная, непрерывная оператор-функция, такая, что* $||\Phi(t)|| \le k_4$, $t \in \mathcal{T}$.

НЕКОТОРЫЕ ОЦЕНКИ СЛОЖНОСТИ ПАРАЛЛЕЛЬНЫХ ПРЕФИКСНЫХ СХЕМ

И. С. Сергеев (Москва)

Рассмотрим задачу реализации системы функций

$$x_1 \circ \ldots \circ x_i, \qquad 1 \le i \le m, \tag{1}$$

которую принято называть системой *префиксов* (или *префиксных сумм*), схемами из функциональных элементов над базисом $\{\circ\}$, где $\circ$ — произвольная бинарная ассоциативная операция.

Обозначим через $L(m)$ сложность минимальной схемы глубины $\lceil \log_2 m \rceil$, реализующей систему функций (1). Понятия глубины и сложности схем из функциональных элементов см. в [1].

В 1978 г. Ладнер и Фишер [5] получили верхнюю оценку $L(m) \le (4 - o(1))m$. В случае $m = 2^n$ была указана более точная оценка

$$L(2^n) \le 4 \cdot 2^n - \Phi_{n+5} + 1,$$

где Φ_k — k-е число Фибоначчи.

Чуть позже Фич [2, 3] получила следующие нижнюю и верхнюю оценки сложности:

$$\left(3\tfrac{1}{3} - o(1)\right) 2^n \le L(2^n) \le \left(3\tfrac{421}{792} - o(1)\right) 2^n.$$

Нижняя оценка относится к универсальной префиксной схеме, т.е. реализующей (1) с любой операцией $\circ$.

В работах [2, 3, 5] также изучалась сложность $L(m, k)$ реализации (1) с глубиной $\lceil \log_2 m \rceil + k$. Содержательным является случай $k \le \log_\varphi m - \log_2 m - O(1)$, где $\varphi = \frac{\sqrt{5}+1}{2}$. Для бóльших значений k ответ $L(m, k) = 2m - k - \lceil \log_2 m \rceil - 2$ дает конструкция [6].

Как в [5], так и в [2, 3] строились схемы, дополнительно удовлетворяющие соглашению реализации максимального префикса $x_1 \circ \ldots \circ x_m$ с минимально возможной глубиной $\lceil \log_2 m \rceil$. Сложность реализации системы (1) схемами из этого класса обозначим через $L'(m, k)$.

В работе [5] были доказаны оценки

$$L'(m,k) < (2+2^{1-k})m-2, \qquad L'(2^n,k) \le (2+2^{1-k})2^n-\Phi_{n+5-k}-k+1,$$

а в работах [2, 3]:

$$\left(2 + \tfrac{1}{3}2^{1-k} - o(1)\right) 2^n \le L'(2^n,k) \le \left(2 + \tfrac{421}{792}2^{1-k} - o(1)\right) 2^n - k.$$

Технически обусловленной является задача синтеза префиксных схем с ограниченным ветвлением элементов. (Задается ограничение q на степень ветвления входов и элементов схемы, при этом степень ветвления выходов не должна превышать $q - 1$.) При построении таких схем помимо функциональных элементов $\circ$ используются также тождественные элементы, которые используются в качестве элементов ветвления. Для обозначения сложности префиксных схем с ограничением q на степень ветвления элементов будем использовать введенные ранее обозначения сложности с нижним индексом q.

Фич [2, 3] показала, что $L_q(m) = \Theta(m)$ при $q \ge 3$ и $L_2(m) = \Theta(m \log m)$. При этом для $m = 2^n$ были получены соотношения

$$(n + 1 - o(1))2^{n-1} \le L_2(2^n) \le (3n - 3,5 - o(1))2^{n-1},$$

$$L'_2(2^n,k) \le (2n - 2k - 3 - o(1))2^{n-k} + 5 \cdot 2^{n-1} - k.$$

Лучшие верхние оценки

$$L_2(2^n) \le (n - 0,5)2^n, \qquad L'_2(2^n,k) \le (n-k-3)2^{n-k} + 5 \cdot 2^{n-1} - k.$$

получаются более ранним методом Коге—Стоуна 1973 г. [4] (вторая — подстановкой схемы Коге—Стоуна в конструкцию Ладнера—Фишера).

К перечисленным результатам можно добавить следующие. Введем обозначения $L^{\oplus}(m)$ и $L'^{\oplus}(m,k)$ для сложности реализации (1) с операцией $\oplus$ сложения по модулю 2, аналогичные обозначениям $L(m)$ и $L'(m,k)$. Справедлива

Теорема.

1) $L(2^n) = 3,5 \cdot 2^n - (8,5 + 3,5(n \bmod 2))2^{\lfloor n/2 \rfloor} + n + 5$;

2) $L(m) \leq (3,5 - o(1))m$;

3) *При* $1 \leq k \leq n-2$ *имеет место соотношение*

$$L'(2^n,k) = (2+2^{-k})2^n - (5 + 2((n-k) \bmod 2))2^{\lfloor (n-k)/2 \rfloor} - k + 2;$$

4) *Для любых* m, k, *где* $1 \leq k \leq \lceil \log_2 m \rceil - 2$, *при* $m \to \infty$ *справедливо* $L'(m,k) \leq (2 + 2^{-k} - o(1))m$;

5) $L^{\oplus}(2^n) \leq 3\frac{3}{11} \cdot 2^n - \tau_n$, *где* $\tau_n = \frac{\sigma_{n+3}+\sigma_{n+2}+\sigma_{n+1}-\sigma_n-n-7}{2}$, *а* σ_n *определяется из рекуррентного соотношения* $\sigma_n = 2\sigma_{n-3} + \sigma_{n-4} + 1$ *с начальными условиями* $\sigma_0 = \frac{25}{11}$, $\sigma_1 = \frac{39}{11}$, $\sigma_2 = \frac{56}{11}$, $\sigma_3 = \frac{79}{11}$;

6) $L^{\oplus}(m) \leq \left(3\frac{3}{11} - o(1)\right) m$;

7) *Для любых* m, k, *где* $1 \leq k \leq \lceil (\log_2 m)/2 \rceil - 1$, *при* $m \to \infty$ *справедливо* $L'^{\oplus}(m,k) \leq \left(2 + \frac{3}{11} \cdot 4^{1-k} - o(1)\right) m$;

8) $L'_2(2^n,k) \leq (n-k-3,25)2^{n-k} + 5 \cdot 2^{n-1} - k$ *при* $n \geq k \geq 1$.

Автор выражает благодарность научному руководителю С. Б. Гашкову за внимание к работе.

Работа выполнена при финансовой поддержке РФФИ (проекты 08–01–00863 и 08–01–00632), программы поддержки ведущих научных школ РФ (проект НШ–4437.2010.1) и программы фундаментальных исследований ОМН РАН «Алгебраические и комбинаторные методы математической кибернетики и информационные системы нового поколения».

Список литературы

1. Лупанов О. Б. Асимптотические оценки сложности управляющих систем. — М.: Изд. МГУ, 1984.

2. Fich F. E. Two problems in concrete complexity: cycle detection and parallel prefix computation. — IBM research report RJ 3651, 1982. (Ph. D. thesis. — Univ. of California, Berkeley, 1982.)

3. Fich F. E. New bounds for parallel prefix circuits // Proc. ACM Symp. Theory of Comput. — 1983. — P. 100–109.

4. Kogge P. M., Stone H. S. A parallel algorithm for the efficient solution of a general class of recurrence equations // IEEE Trans. on Comp. — 1973. — V. 22, № 8. — P. 786–793.

5. Ladner R. E., Fischer M. J. Parallel prefix computation // J. ACM. — 1980. — V. 27, № 4. — P. 831–838.

6. Zhu H., Cheng C.-K., Graham R. Constructing zero-deficiency parallel prefix circuits of minimum depth // Proc. ASP-DAC. — 2005. — P. 883–888.

О НИЖНИХ ОЦЕНКАХ ГЛУБИНЫ ФОРМУЛ СПЕЦИАЛЬНОГО ВИДА

Д. В. Трущин (Москва)

В работе рассматривается задача о реализации булевых функций α-формулами — формулами специального вида, в которых каждая подформула содержит не более одной нетривиальной главной подформулы. В качестве меры сложности формул рассматривается глубина. Получены нижние оценки функций Шеннона для α-пополнений некоторых конечных систем булевых функций.

Множество всех булевых функций обозначим через P_2, множество всех монотонных булевых функций — через M, а через $H(n)$, $H \subseteq P_2$, — множество функций, принадлежащих множеству H и зависящих только от переменных $x_1, \ldots, x_n$.

Пусть $\mathfrak{A}$ — конечная система функций из P_2, а Φ — некоторая формула над $\mathfrak{A}$. *Сложностью* $L(\Phi)$ этой формулы называется число символов переменных, входящих в нее. *Глубину* $D(\Phi)$ формулы Φ определим индуктивно. Если Φ состоит только из символа переменной, то $D(\Phi) = 0$. Если Φ имеет вид $f(\Phi_1, \ldots, \Phi_m)$, где $f \in \mathfrak{A}$, а $\Phi_1, \ldots, \Phi_m$ — формулы над $\mathfrak{A}$, то положим $D(\Phi) = 1 + \max D(\Phi_i)$, где максимум берется по всем $i = 1, \ldots, m$. Для любой функции $f \in [\mathfrak{A}]$ положим $L_{\mathfrak{A}}(f) = \min L(\Phi), D_{\mathfrak{A}}(f) = \min D(\Phi)$, где каждый минимум берется по всем формулам Φ над $\mathfrak{A}$, реализующим f.

Следуя [1], определим индуктивно понятие α-*формулы* Φ над конечной системой $\mathfrak{A}$ булевых функций. Символ переменной является элементарной α-формулой. Если ϕ — α-формула над $\mathfrak{A}$, f — символ

m–местной функции из $\mathfrak{A}$, $m \geq 1$, а $x_{i_2}, \ldots, x_{i_m}$ — символы переменных, то выражение $f(\phi, x_{i_2}, \ldots, x_{i_m})$ также является α-формулой. Множество всех функций, реализуемых α-формулами над $\mathfrak{A}$, будем называть α-*пополнением* системы $\mathfrak{A}$ и обозначать через $[\mathfrak{A}]_\alpha$. Система $\mathfrak{A} \subset P_2$ называется α-*полной*, если $[\mathfrak{A}]_\alpha = P_2$.

Пусть $\mathfrak{A}$ — конечная система булевых функций, $f \in [\mathfrak{A}]_\alpha$. Положим $D^\alpha_\mathfrak{A}(f) = \min D(\Phi)$, $L^\alpha_\mathfrak{A}(f) = \min L(\Phi)$, где каждый минимум берется по всем α-формулам Φ над $\mathfrak{A}$, реализующим f. Будем называть α-формулу Φ *минимальной* (для функции f), если Φ реализует f, и $D(\Phi) = D^\alpha_\mathfrak{A}(f)$. Определим *функцию Шеннона* следующим образом. Положим $D^\alpha_\mathfrak{A}(n) = \max D^\alpha_\mathfrak{A}(f)$, где максимум берется по всем функциям $f \in H(n)$, $H = [\mathfrak{A}]_\alpha$. Не сложно видеть, что для введенных мер сложности справедливы неравенства $c_1 D^\alpha_\mathfrak{A}(f) \leq L^\alpha_\mathfrak{A}(f) \leq c_2 D^\alpha_\mathfrak{A}(f)$, где c_1 и c_2 — константы, зависящие от $\mathfrak{A}$.

Пусть $f(x_1, \ldots, x_n)$ — произвольная булева функция. Обозначим число аргументов функции f через $m(f)$. Для всякой конечной системы $\mathfrak{A} \subset P_2$ положим $m(\mathfrak{A}) = \max m(f)$, $p(\mathfrak{A}) = \max m(f)$, где максимумы берутся по всем функциям из множеств $\mathfrak{A}$ и $\mathfrak{A} \setminus M$ соответственно. При этом если $\mathfrak{A} \subset M$, считаем, что $p(\mathfrak{A}) = 1$.

В работе [2] автором показано, что если $\mathfrak{A}$ — произвольная конечная система булевых функций, и функция $f^{(n)}(x_1, \ldots, x_n)$ принадлежит $[\mathfrak{A}]_\alpha$, то имеет место неравенство

$$D^\alpha_\mathfrak{A}(f^{(n)}) \leq cn^r,$$

где $r = m(\mathfrak{A}) + p(\mathfrak{A}) - 2$, c — некоторая константа, зависящая от $\mathfrak{A}$. Из этой оценки следует, что в P_2 не существует конечных систем, являющихся α-полными (см. также [2, 3]). Следует отметить, что при всех $k \geq 3$ в P_k существуют конечные α-полные системы [1, 3, 4].

Также в работе [2] показано, что при любом натуральном $p \geq 2$ существует конечная система монотонных булевых функций $\mathfrak{A}$ такая, что

$$c_1 n^p \leq D^\alpha_\mathfrak{A}(n) \leq c_2 n^p,$$

где c_1 и c_2 — константы, зависящие от $\mathfrak{A}$, $n \geq p$. Таким образом, приведенная верхняя оценка, вообще говоря, неулучшаема с точностью до порядка для систем монотонных булевых функций.

Положим $\mathfrak{A} = \{x + y, xy, \overline{x}\}$.

Индуктивно определим для любого $n \geq 1$ функцию $f_n(x_1, \ldots, x_n)$ следующим образом. Положим $f_1(x_1) = x_1$ и

$$f_n(x_1, \ldots, x_n) = f_{n-1}(x_1, \ldots, x_{n-1})\&x_n + x_1 + x_2 + \ldots + x_n$$

при всех $n \geq 2$. Не сложно заметить, что $f_n \in [\mathfrak{A}]_\alpha$.

Лемма. *Для любого $n \geq 1$ справедливо равенство*

$$D^\alpha_{\mathfrak{A}}(f_n) = \frac{(n+1)(n+2)}{2} - 3.$$

Теорема. *При любых $n \geq 1$ справедливы неравенства*

$$c_1 n^2 \leq D^\alpha_{\mathfrak{A}}(n) \leq c_2 n^2,$$

где c_1, c_2 — положительные константы, не зависящие от n.

Таким образом приведен пример системы, содержащей немонотонные функции, для которой полученная в [2] верхняя оценка также является наилучшей с точностью до порядка.

В заключение автор выражает искреннюю признательность А.Б. Угольникову за постановку задачи и обсуждение результатов работы.

Работа выполнена при финансовой поддержке РФФИ (проект 08–01–00863), программы поддержки ведущих научных школ РФ (проект НШ–4437.2010.1) и программы фундаментальных исследований ОМН РАН «Алгебраические и комбинаторные методы математической кибернетики и информационные системы нового поколения».

Список литературы

1. Глухов М. М. Об α-замкнутых классах и α-полных системах функций k–значной логики // Дискретная математика. — 1989. — Т. 1, вып. 1. — С. 16–21.

2. Трущин Д. В. О глубине α-пополнений систем булевых функций // Вестник Московского университета. Сер. 1. Математика. Механика. — 2009. — Вып. 2. — С. 72–75.

3. Чернышов А. Л. Условия α-полноты систем функций многозначной логики // Дискретная математика. — 1992. — Т. 4, вып. 4. — С. 117–130.

4. Шабунин А. Л. Примеры α-полных систем k–значной логики при $k = 3, 4$ // Дискретня математика. — 2006. — Т. 18, вып. 4. — С. 45–55.

К ОПТИМИЗАЦИИ НЕНАДЕЖНЫХ СИСТЕМ

А. В. Угланов (Санкт-Петербург),
В. А. Бадоев (Ярославль)

Работа относится к прикладной теории вероятностей (оптимизационная компонента здесь тривиальна). Результаты представляют интерес, в частности, для инженерии (например, при нахождении оптимальной конструкции сложных технологических цепочек: см. [1], где одна такая конструкция найдена, но лишь приближенно).

Постановка задач. Система состоит из n ненадежных элементов, m из которых — рабочие ($m \leq n$), а $n-m$ — резервные. Рабочие элементы функционируют независимо друг от друга показательно распределенное с параметром λ случайное время, после чего выходят из строя. Резервные элементы непосредственно из строя не выходят (ненагруженный резерв), а служат для замены рабочих: в случае отказа рабочего элемента он немедленно заменяется резервным, если таковой еще имеется; если же резерв исчерпан, то происходит остановка работы всей системы (авария), которая ликвидируется за время $(n-m+1)t_0$ с затратами $a(n-m+1)$ (t_0, $a \geq 0$ суть соответственно время ремонта одного элемента и затраты на этот ремонт). Во время ликвидации аварии элементы из строя не выходят, и в момент окончания ликвидации все n элементов исправны. Периодически, с периодом τ, осуществляются профилактики при которых восстанавливаются все вышедшие иэ строя элементы ($0 < \tau \leq \infty$; равенство $\tau = \infty$ означает отсутствие профилактик — мы не исключаем и этот случай). Продолжительность каждой профилактики есть $t_p \geq 0$, и в течение этого времени система работает. Затраты на каждую профилактику есть $b \geq 0$. Если авария произошла в такой момент, что время до очередной профилактики меньше $(n-m+1)t_0$, то аварийный ремонт не производится (ожидается профилактика). Предполагается, что $(n-m+1)t_0 \leq t_p \leq \tau$. Обозначим через $T_w(T)$ и D_T соответственно время работы системы и ремонтные затраты на временно́м промежутке $[0, T]$ (T называется периодом эксплуатации) и положим

$$R(T) = \frac{\mathsf{E}T_w(T)}{T}, \quad D(T) = \frac{\mathsf{E}D_T}{T}$$

(E — знак математического ожидания). $R(T)$ есть надежность системы при периоде эксплуатации T. На практике T велико (математически: $\lambda T >> 1$), так что представляет интерес предельное (при $T \to \infty$) поведение величин $R(T)$, $D(T)$.

Задача 1 (вероятностная): доказать существование пределов

$$R \stackrel{\text{def}}{=} \lim_{T\to\infty} R(T), \quad D \stackrel{\text{def}}{=} \lim_{T\to\infty} D(T), \tag{1}$$

и найти эти пределы. Пусть задача решена и пусть V есть (конечное) множество всех допустимых способов конструирования системы. Тогда, естественно, параметры λ, t_0, t_p, a, b суть (известные) функции от $v \in V$; тогда и величины R, D суть функции от v. Положим

$$F : V \to R^1 : F(v) = KR(v) - D(v), \tag{2}$$

где K некоторый (известный) коэффициент, определяемый выгодой от увеличения надежности системы.

Задача 2 (экстремальная): найти v, при котором функция F достигает максимума.

Результаты. Введем обозначение

$$s_+^j = \begin{cases} s^j, & \text{если } s \geq 0 \quad (0^0 = 1), \\ 0, & \text{если } s < 0, \end{cases}$$

и величины:

$$P_{i,j} = e^{-m\lambda(\tau - t_p - j(n-m+1)t_0)} \times$$
$$\times \frac{(m\lambda)^{(n-m+1)j+i}}{((n-m+1)j+i)!}(\tau - t_p - j(n-m+1)t_0)_+^{(n-m+1)j+i},$$

где $i = 1, \ldots, n-m$, $j = 0, 1, \ldots$; если $n = m$, то $P_{i,j} = 0$;

$$P_i = \sum_{j=0}^{\mathsf{int}} P_{i,j}$$

$\Big($здесь и ниже int есть целая часть числа $\left[\frac{\tau - t_p - 0}{(n-m+1)t_0}\right]\Big)$;

$$P_{n-m+1} = \sum_{l=1}^{\mathsf{int}+1} \int_{\tau-(n-m+1)t_0}^{\tau} e^{-m\lambda(t-(l-1)(n-m+1)t_0)} \times$$
$$\times \frac{(m\lambda)^{l(n-m+1)}[t-(l-1)(n-m+1)t_0]_+^{l(n-m+1)-1}}{((l(n-m+1)-1)!}\,dt;$$

$$E_0 = \sum_{l=1}^{\mathsf{int}+1} \int_{\tau-(n-m+1)t_0}^{\tau} (\tau - t) e^{-m\lambda(t-(l-1)(n-m+1)t_0)} \times$$

$$\times \frac{(m\lambda)^{l(n-m+1)} [t-(l-1)(n-m+1)t_0]_+^{l(n-m+1)-1}}{((l(n-m+1)-1)!} \, dt;$$

$$E_1 = \sum_{l=1}^{n-m+1} l P_l \, .$$

Замечание 1. Введенные величины имеют совершенно определенный и достаточно интересный вероятностный смысл, но мы не имеем здесь возможности останавливаться на этом вопросе.

Теорема. *Пределы* (1) *существуют и справедливы равенства*

$$R = 1 - \frac{E_0 + (m\lambda(\tau - t_p) - E_1)t_0}{(1 + m\lambda t_0)\tau}, \tag{3}$$

$$D = a\frac{m\lambda(\tau - t_p - E_0) - E_1)}{(1 + m\lambda t_0)\tau} + b\frac{E_1}{\tau}. \tag{4}$$

Замечание 2. Получение равенств (3), (4) достаточно сложно (так, нам пришлось вычислять статистические характеристики функций двух аргументов — случайного множества и случайного процесса, причем аргументы эти зависимы).

Поскольку равенства (3), (4) дают явное выражение для целевой функции (2), то максимизация этой функции может быть осуществлена простым перебором.

Работа второго автора выполнена при финансовой поддержке Российского фонда фундаментальных исследований (проект 09-01-00677).

Список литературы

1. Kononova A . V., Neri F., Semoushin I., Uglanov A. V. Analysis of one complex unreliable system // Next generation concurrent engineering. Smart and concurrent integration of poroduct data, services and control. — International society for productivity. — Enhancement. — ISPE, V. 1. — Ft. Worth (USA), 2005. — P. 397–400.

КОДИРОВАНИЕ ПОТОКА СБОЕВ И НАДЕЖНОСТЬ УПРАВЛЯЮЩИХ СИСТЕМ

М. А. Федоткин, А. М. Федоткин (Нижний Новгород)

В работе изучены случайные последовательности из моментов сбоев управляющих систем [1–4], функционирующих в экстремальных условиях. При этом предполагается, что каждая управляющая система построена, а сбои происходят как за счет изменения внешней среды, так и за счет ненадежности функционирования ее элементов. В этом случае интервалы между последовательными сбоями элементов системы являются зависимыми и имеют различные распределения. Поэтому не удается найти конечномерные распределения числа сбоев элементов управляющей системы за произвольный момент времени t. Предложен нетрадиционный способ кодирования последовательности сбоев или потока сбоев такой сложной вероятностной структуры. Этот способ основан на выделении сбоев так называемых главных элементов системы. При этом сбой каждого из главных элементов порождает группу новых сбоев других элементов. На примерах функционирования большого числа реальных управляющих систем проведен статистический анализ как последовательностей из моментов сбоев главных элементов, так и числа всех типов сбоев за промежуток времени между двумя последовательными сбоями главных элементов. Результаты такого статистического анализа позволяют рекомендовать простой метод контроля за функционированием системы, который значительно уменьшает дисперсию числа сбоев всех типов элементов до момента t.

Обозначим через $\{\tau'_i;\ i \geq 1\}$ последовательность из моментов сбоев всех типов элементов системы. Пусть теперь $\tau_0 = \tau'_1$ и $\{\tau_i;\ i \geq 0\}$ есть строго возрастающая последовательность из моментов появления сбоев главных элементов. Так как i-ый момент $\tau_i = \tau'_{k_i}$ при $i \geq 0$, $k_i \in \{1, 2, ...\}$, $k_0 = 1$, то случайная величина $\eta_i = k_{i+1} - k_i$ определяет число всех наблюдаемых сбоев на промежутке времени $[\tau_i, \tau_{i+1})$. Отсюда следует, что необходимо предложить такой алгоритм выбора целочисленных случайных величин $\{k_i;\ i \geq 0\}$, который позволяет идентифицировать распределение вспомогательной векторной последовательности $\{(\tau_i, \eta_i);\ i \geq 0\}$. При положительном решении последней задачи кодирование потока сбоев естественно выполнять в виде векторной последовательности $\{(\tau_i, \eta_i);\ i \geq 0\}$. Приведем один из алгоритмов построения последовательности $\{k_i;\ i \geq 0\}$.

Пусть при $c = 0, 1, ...$ моменты $\tau_i^{(c)} < \tau_{i+1}^{(c)}$, $i \geq 0$, совпадают с некоторыми элементами последовательности $\{\tau'_i;\ i \geq 1\}$, т. е. величина

$\tau_i^{(c)} = \tau'_{k_{c,\,i}},\ k_{c,i} \in \{1, 2, ...\}$. Тогда величина $\eta_i^{(c)} = k_{c,i+1} - k_{c,i}$ задает число всех типов сбоев на промежутке $[\tau_i^{(c)}, \tau_{i+1}^{(c)})$. При новом описании исходного потока $\{\tau'_i;\ i \geq 1\}$ сбоев в виде последовательности $\{(\tau_i^{(c)}, \eta_i^{(c)});\ i \geq 0\}$ величину $\eta_i^{(c)}$ назовем $i-$ой группой, а величину $\delta_i^{(c)} = \tau'_{k_{c,i+1}} - \tau'_{k_{c,i+1}-1}$ интервалом между последовательными группами $\eta_i^{(c)}, \eta_{i+1}^{(c)}$. Моменты $\tau_i^{(c)},\ c \geq 0,\ i \geq 0$, будем строить с помощью рекуррентных соотношений: $k_{0,i+1} = \inf\{j :\ j > k_{0,i},\ \tau'_j - \tau'_{j-1} \geq h_0\}$, $s_c = \inf\{j :\ \ j \geq 0,\ \eta_j^{(c)} \leq d,\ \eta_{j+1}^{(c)} \leq d,\ \delta_j^{(c)} < h_1, \eta_j^{(c)} = \eta_{j-1}^{(c)}\}$, $\tau_i^{(c+1)} = \tau_i^{(c)}$ при $i \leq s_c$ и $\tau_i^{(c+1)} = \tau_{i+1}^{(c)}$ при $i > s_c$. В этих формулах при каждом $c = 0, 1, ...$ величина $\eta_{-1}^{(c)} = 1$, $k_{0,0} = 1$, d — некоторое натуральное число, а постоянные величины h_0, h_1 удовлетворяют условию $h_0 < h_1$.

Этот алгоритм выбора последовательностей $\{(\tau_i^{(c)}, \eta_i^{(c)});\ i \geq 0\}$, $c = 0, 1, ...$, используя величину h_0, сначала разбивает исходный процесс $\{\tau'_i;\ i \geq 1\}$ на группы с целью получения маркированного точечного процесса $\{(\tau_i^{(0)}, \eta_i^{(0)});\ i \geq 0\}$ нулевого уровня. Далее, последовательно, начиная с нулевой группы $\eta_0^{(0)}$, алгоритм объединяет первые две соседние группы $\eta_j^{(0)}$ и $\eta_{j+1}^{(0)}$, если каждая из них содержат не более d сбоев, интервал между такими группами строго меньше величины h_1 и, наконец, выполняется равенств $\eta_j^{(0)} = \eta_{j-1}^{(0)}$. Это позволяет найти процесс $\{(\tau_i^{(1)}, \eta_i^{(1)});\ i \geq 0\}$ первого уровня, к которому применяем ту же самую процедуру, что и к процессу $\{(\tau_i^{(0)}, \eta_i^{(0)});\ i \geq 0\}$. В результате получаем маркированный точечный процесс $\{(\tau_i^{(2)}, \eta_i^{(2)});\ i \geq 0\}$ второго уровня и т. д.

Теорема. *Для любой реализации* $\omega = \{t'_i;\ i \geq 1\}$ *случайной последовательности* $\{\tau'_i;\ i \geq 1\}$ *и для любого фиксированного* $i \geq 0$ *существуют пределы* $\lim_{c\to\infty} k_{c,i}(\omega)$, $\lim_{c\to\infty} \tau_i^{(c)}(\omega)$.

Данная теорема позволяет для любого $i \geq 0$ определить случайные величины $k_i = \lim_{c\to\infty} k_{c,i}$, $\tau_i = \lim_{c\to\infty} \tau_i^{(c)}$. При таком алгоритме выбора потока $\{(\tau_i, \eta_i);\ i \geq 0\}$ имеем $\tau_i = \tau'_{k_i}$, $\eta_i = k_{i+1} - k_i$ для всех $i \geq 0$ и, следовательно, таким способом определяем число всех сбоев управляющей системы на промежутке времени $[\tau_i, \tau_{i+1})$. Используя статистические данные из [5, 6] и различные критерии проверки гиеотез из [7], было установлено, что при сответствующем

подборе постоянных d, h_0, h_1 как случайные величины $\tau_i,\ i \geq 0$, так и случайные величины $\eta_i,\ i \geq 0$, будут независимыми и одинаково распределенными. Более того определены распределения случайных величин $\tau_{i+1} - \tau_i$, η_i. Используя вид распределений случайных величин $\tau_{i+1} - \tau_i$, η_i и их независимость, разработан способ профилактики главных элементов управляющей системы, который приводит к повышению надежности ее функционирования.

Работа выполнена в Нижегородском государственном университете им. Н. И. Лобачевского при финансовой поддержке госбюджетной НИР, проводимой по заданию Федерального агентства по образованию по теме "Анализ дискретных управляющих систем обслуживания и систем вычисления булевых функций" (номер государственной регистрации 01.2.00 6 02598).

Список литературы

1. Ляпунов А. А., Яблонский С. В. Теоретические проблемы кибернетики // Проблемы кибернетики. Вып. 9. — 1963. — С. 5–22.

2. Федоткин М. А. Процессы обслуживания и управляющие системы // Мат. вопросы кибернетики. Вып. 6. — 1996. — С. 51–70.

3. Федоткин М. А. Нелокальный способ задания управляемых случайных процессов // Мат. вопросы кибернетики. Вып. 7. — 1998. — С. 332–344.

4. Федоткин М. А. О моделях случайных экспериментов с управлением // Abstracts of International Conference on "Kolmogorov and Contemporary Mathematics". — М: МГУ, 2003. — С. 656–657.

5. Кокс Д., Льюис П. Статистический анализ последовательностей событий. — М.: Мир, 1969.

6. Bartlett M. S. The spectral analysis of point processes // J. R. Statist. Soc. B. — 1963. — V. 25, №. 2. — P. 264–296.

7. Fedotkin A. M., Fedotkin M. A. Model for refusals of elements of a controlling system // Transactions of the first French-Russian Conference on "Longevity, Aging and Degradation Models in Reliability, Public Health, Medicine and Biology, LAD' 2004". — St. Petersburg: St. Petersburg State Politechnical University, 2004. — V. 2. — P. 136–151.

НИЖНИЕ ОЦЕНКИ ДЛЯ БУЛЕВЫХ ФУНКЦИЙ В ПРЕДСТАВЛЕНИИ РАЗЛИЧНЫМИ МОДЕЛЯМИ k-OBDD

К. Р. Хадиев (Казань)

Мы рассматриваем модель ветвящейся программы (ВР — branching program), определенную в книге [5].

В данной работе представлена техника доказательства нижних оценок реализации булевых фукций в различных моделях k-$OBDD$, которые являются известными представителями ветвящихся программ.

Ветвящаяся программа называется *уровневой*, если ее вершины могут быть разбиты на уровни $0, 1, \ldots$ таким образом, что для каждого i ребра из вершин уровня i ведут только в вершины уровня $(i+1)$.

Ширина $w(P)$ уровневой ветвящейся программы P — это максимум от количества вершин на уровне, взятый по всем уровням программы P.

Уровневая ветвящаяся программа P называется *забывающей*, если на любом уровне P тестируется только одна переменная.

Уровневая ветвящаяся программа P называется один раз читающей, если на любом пути вычисления каждая переменная читается один раз.

Упорядоченное дерево решений ($OBDD$) на множестве переменных $X_n = \{x_1, x_2, \ldots, x_n\}$ — это уровневая забывающая один раз читающая ветвящаяся программа.

Говорят, что $OBDD$ читает переменные в некотором порядке π, где π — перестановка чисел от 1 до n. Если чтение происходит в этом порядке k раз, то такая модель называется k-$OBDD$.

Порядок π=$(1, \ldots, n)$, называется id, и $OBDD$, которая читает переменные в этом порядке обозначается id-$OBDD$, если модель k раз читающая, то для нее введем обозначение k-id-$OBDD$.

Для k-$OBDD$, $k \geq 2$, пусть $\pi_1 = (1, \ldots, n)$, $\pi_2 = (n, \ldots, 1)$ — два порядка считывания переменных. Если k-$OBDD$ читает переменные в порядке $\pi_1\pi_2\pi_1\pi_2\ldots$, такую k-$OBDD$ называют k-$sweeping$-$OBDD$.

Обозначим за k-$OBDD_w$ множество функций, распознаваемых k-$OBDD$ с шириной w. За k-id-$OBDD_w$ и k-$swepping$-$OBDD_w$ множество функций, распознаваемых k-id-$OBDD$ с шириной w и k-$swepping$-$OBDD$ с шириной w соответственно.

Рассмотрим переменные $x_1, \ldots, x_n$. Разобьем их на 2 множества $x_1, \ldots, x_m$ и $x_{m+1}, \ldots, x_n$. Возьмем два булевых вектора длины m

$\sigma_1 \dots \sigma_m$ и $\sigma'_1 \dots \sigma'_m$. Тогда если мы подставим вместо первых m переменных эти вектора, то получим две булевы функции над $n-m$ переменными f_σ и $f_{\sigma'}$. В случае, если эти функции равны, наборы $\sigma_1 \dots \sigma_m$ и $\sigma'_1 \dots \sigma'_m$ называются эквивалентными, и используется обозначение $\sigma =_f \sigma'$; f_σ и $f_{\sigma'}$ называются подфункциями функции f.

Обозначим за $\phi_f(m,n)$ количество различных подфункций при фиксировании первых m переменных. Или это количество попарно неэквивалентных наборов $\sigma_1 \dots \sigma_m$.

Назовем количеством различных подфункций фукции f над n переменными число $\phi_f(n) = \max_{m=\{1\dots n\}} \phi_f(m,n)$. При этом m, на котором достигается максимум, обозначим за $N(n)$.

Свойство. Для произвольной булевой функции f над n переменными выполняется следующее неравенство: $\phi_f(n) \le |X|^{n-log(n)}$.

Такое неравенство достигается к примеру на мультиплексорной функции (ISA).

Функция ISA определяется следующим образом. Берутся последние $\log(n)$ переменных. Вычисляется k — число, двоичный вид которого записан в этих переменных. Результатом функции является значение x_k.

Результаты:

Если $f \in k\text{-}id\text{-}OBDD_w$ или $f \in k\text{-}sweeping\text{-}OBDD_w$ тогда $\phi_F(n) \le O(w^w)$.

Если $f \in k\text{-}id\text{-}OBDD_{const}$ или $f \in k\text{-}sweeping\text{-}OBDD_{const}$ тогда $\phi_F(n) \le const$.

Если $f \in k\text{-}id\text{-}OBDD_{\log(n)}$ или $f \in k\text{-}sweeping\text{-}OBDD_{\log(n)}$ тогда $\phi_F(n) \le O(N^{O(\log\log(n))})$.

Эти результаты дают достаточное условие непредставимости функций в указанных моделях $k\text{-}OBDD$. Рассмотрим несколько примеров:

1. Функция равенства двух половин входного набора EQU, равная 1 только на $\{xx : x \in \{0,1\}^{n/2}\}$. Для нее наибольшее число подфункций образуется, если мы разделим набор переменных ровно посередине, тогда $N(n) = n/2$, $\phi(n) = 2^N = 2^{n/2}$, так как каждая подстановка $\sigma_1 \dots \sigma_N$ для переменных $x_1 \dots x_N$ будет порождать собственную подфункцию, котора будет давать 1 только в случае, когда $x_{N+1} = \sigma_1, \dots x_n = \sigma_N$. Такая функция не может быть распознана ни одной из представленных моделей.

2. Функция ISA также не реализуема ни одной из рассматриваемых моделей.

3. Функция равенства 0 и 1 во входном наборе переменных O, равная 1 только на наборах $\{x \in \{0,1\}^n : \sharp_0(x) = \sharp_1(x)\}$, где $\sharp_r(x)$ — количество символов r в слове x. Для нее наибольшее число подфункций образуется, если мы разделим набор переменных ровно по середине, тогда $N(n) = n/2$, $\phi(n) = N = n/2$, так как различные подфункции образуют только подстановки в которыех различное число единиц. Можно сказать, что $O \notin k\text{-}id\text{-}OBDD_{const}$, $k\text{-}sweeping\text{-}OBDD_{const}$.

Список литературы

1. Condon A. Bounded error probabilistic finite state automata.

2. Dwork C., Stockmeyer L., A time-complexity gap for two-way probabalistic finite state automata // SIAM J. Comput. — 1990. — V. 19. — P. 1011–1023.

3. Leighton F. T., Rivest R. L. Estimating a probability using finite memory // IEEE Transactions on Information Theory. — 1986. — V. IT-32, № 6.

4. Shepherdson J. The reduction of two-way automata to one-way automata // IBM Journal of Research and Development. — 1959. — V. 3. — P. 198–200.

5. Wegener I. Branching programs and binary decision diagrams: theory ans applications // Society for Industrial and Applied Mathematics. — Philadelphia, 2000.

6. Lee C. Y. Representation of switching circuits by binary-decision programs // Bell Systems Technical Journal. — 1959. — V. 39. — P. 985–999.

ИССЛЕДОВАНИЕ СЛОЖНОСТИ УМНОЖЕНИЯ В КОММУТАТИВНЫХ ГРУППОВЫХ АЛГЕБРАХ

Б. В. Чокаев (Москва)

Одной из центральных областей алгебраической теории сложности является сложность умножения в алгебрах. Алгеброй называется линейное пространство, наделенное операцией умножения: отображением, которое двум произвольным элементам пространства ставит в соответствие определенный элемент этого пространства, причем это отображение является линейным по обоим аргументам. При этом размерность линейного пространства называется размерностью алгебры, базис пространства — базисом алгебры. Задача сложности умножения в алгебре заключается в том, чтобы построить алгоритм, принадлежащий заранее зафиксированному классу

алгоритмов, который для любых двух элементов этой алгебры вычислял бы их произведение и имел бы наименьшую сложность среди всех алгоритмов данного класса. Общепринятым в алгебраической теории сложности является класс билинейных алгоритмов [4].

Определение. *Билинейным алгоритмом умножения* для алгебры A называется такая последовательность $(f_1, g_1, w_1, \ldots, f_r, g_r, w_r)$, где $f_\rho, g_\rho \in A^*, w_\rho \in A,\ 1 \le \rho \le r$, что для любых векторов $a, b \in A$

$$a \cdot b = \sum_{\rho=1}^{r} f_\rho(a) g_\rho(b) w_\rho.$$

Число r называется *длиной* билинейного алгоритма. *Билинейной сложностью умножения* в алгебре A или *рангом* A называется длина кратчайшего билинейного алгоритма для A и обозначается $\mathrm{rk}A$.

Теорема [1]. *Для произвольной ассоциативной алгебры A выполняется*

$$\mathrm{rk}A \ge 2 \dim A - t(A),$$

где $t(A)$ — число максимальных двусторонних идеалов A. Алгебры, для которых эта оценка совпадает с верхней, называются *алгебрами минимального ранга.*

Определение. Алгебра A называется *групповой алгеброй,* если существует такой базис $a_1, \ldots, a_n$ этой алгебры, что множество $\{a_1, \ldots, a_n\}$ образует некоторую группу G относительно умножения в A. В этом случае алгебра A обозначается $F[G]$, где F — поле над которым она определена.

Сложность умножения в групповых алгебрах оказалась тесно связанной со сложностью умножения в алгебре матриц. В 2003 году Генри Коэн и Кристофер Уманс доказали, что, если сложность умножения в групповых алгебрах почти линейна относительно размерности алгебры, то сложность умножения матриц порядка n почти квадратична относительно n [6].

Данная работа посвящена исследованию билинейной сложности умножения в коммутативных групповых алгебрах над произвольными полями. Для решения этой задачи предложен метод нахождения структуры групповых алгебр, который позволяет использовать теорему Алдера—Штрассена для доказательства нижних оценок и теорему Блезера [2], описывающую все алгебры минимального ранга, для доказательства верхних оценок.

При исследовании билинейной сложности алгебры интересным является вопрос о том, является ли данная алгебра алгеброй минимального ранга. Другой интересный вопрос: если алгебра не минимального ранга, то верна ли для неё линейная верхняя оценка на

билинейную сложность. Ответы на эти вопросы существенно отличаются в зависимости от того над каким полем рассматривается алгебра: над полем характеристики 0 или над полем простой характеристики.

Теорема 1. *Пусть* $\mathbb{F}[G]$ *— произвольная коммутативная групповая алгебра размерности* n *над полем характеристики* 0. *Тогда алгебра* $\mathbb{F}[G]$ *является алгеброй минимального ранга, и* $\mathrm{rk}\mathbb{F}[G] = 2n - s$.

Для вычисления числа s найдены несложные формулы, зависящие от структуры группы G, а также от разложения над полем $\mathbb{F}$ двучлена $X^n - 1$ на неприводимые сомножители.

Теорема 2. *Пусть* $\mathbb{F}[G_n]$ *— групповая алгебра группы*

$$G_n \cong \underbrace{\mathbb{Z}_p \times \mathbb{Z}_p \times \ldots \times \mathbb{Z}_p}_{n \text{ раз}}$$

над произвольным полем $\mathbb{F}$ *характеристики* p. *Тогда*

$$\mathrm{rk}\,\mathbb{F}[G_n] \geq (3 - o(1)) \dim \mathbb{F}[G_n], \text{ при } n \to \infty.$$

Таким образом, в отличие от алгебр над полями характеристики 0, над полями простой характеристики существуют коммутативные групповые алгебры, не являющиеся алгебрами минимального ранга.

Заметим, что в теореме 2 получена наилучшая среди известных нижняя оценка билинейной сложности. В работе [3] впервые была построена последовательность явно заданных алгебр A_n с нижней оценкой $(3 - o(1)) \dim A_n$. Теорема 2 показывает, что последовательность алгебр с такой нижней оценкой можно выбрать и среди коммутативных групповых алгебр.

Следующая теорема отвечает на вопрос о справедливости линейной верхней оценки для некоторого класса алгебр над полем простой характеристики. Доказательство этой теоремы основано на известной теореме братьев Чудновских о линейности ранга конечного поля над его подполем [5].

Теорема 3. *Существует константа* C *такая, что для произвольной коммутативной групповой алгебры* $\mathbb{F}[G]$ *размерности* n *над полем характеристики* p, $p \nmid n$, *выполняется:* $\mathrm{rk}\,\mathbb{F}[G] \leq Cn$.

Работа выполнена при финансовой поддержке РФФИ (проект 09-01-00701).

Список литературы

1. Alder A., Strassen V. On the algorithmic complexity of associative algebras // Theoret. Comput. Sci. — 1981. — V. 15. — P. 201–211.

2. Bläser M. Algebras of minimal rank over arbitrary fields // SIAM Technical Report. — May 10, 2002.

3. Bläser M. Improvements of the Alder-Strassen bound: algebras with nonzero radical // Institut für Theoretische Informatik, Germany.

4. Bürgisser P., Clausen M., Shokrollahi M. Algebraic complexity theory. — Springer, 1997.

5. Chudnovsky D., Chudnovsky G. Algebraic complexities and algebraic curves over finite fields // J. Complexity. — 1988. — V. 4. — P. 285–316.

6. Cohn H., Umans C. A group-theoretic approach to fast matrix multiplication // FOCS-2003. — 2003. — P. 438–449.

О РАСШИРЕНИИ МНОЖЕСТВА ФУНКЦИЙ, ПОВЫШАЮЩИХ НАДЕЖНОСТЬ

В. В. Чугунова (Пенза)

Пусть функциональные элементы подвержены инверсным неисправностям на входах. Эти неисправности характеризуются тем, что поступающее на каждый вход элемента значение a ($a \in \{0,1\}$) с вероятностью ε ($0 < \varepsilon < 1/2$) может превратиться в значение $\bar{a}$.

Пусть $P_{\bar{f}(\tilde{a})}(S, \tilde{a})$ — вероятность появления значения $\bar{f}(\tilde{a})$ на выходе схемы S, реализующей булеву функцию $f(\tilde{x})$, при входном наборе $\tilde{a}$. Ненадежность $P(S)$ схемы S определяется как максимальное из чисел $P_{\bar{f}(\tilde{a})}(S, \tilde{a})$ при всевозможных входных наборах $\tilde{a}$. Надежность схемы S равна $1 - P(S)$.

Обозначим $P_\varepsilon(f) = \inf P(S)$, где S — схема из ненадежных элементов, реализующая булеву функцию f. Схему A из ненадежных элементов, реализующую булеву функцию f, назовем асимптотически оптимальной (наилучшей) по надежности, если $P(A) \sim P_\varepsilon(f)$ при $\varepsilon \to 0$.

Опишем функции $h(x_1, ..., x_r)$, образующие множество H_r. Функции $h(x_1, ..., x_r)$ существенно зависят от $2k + 1$ переменных (от остальных переменных возможно зависят несущественно) и имеют характеристические наборы $\tilde{b} = (b_1, ..., b_r)$ и $\bar{\tilde{b}} = (\bar{b}_1, ..., \bar{b}_r)$, такие что:

1) на наборе $\tilde{b} = (b_1, ..., b_r)$ и на всех наборах $\tilde{a} = (a_1, ..., a_r)$, таких, что расстояние Хэмминга между ними не более k, т.е.

$$\rho(\tilde{a}, \tilde{b}) = \sum_{i=1}^{2k+1} |a_i - b_i| \leq k,$$

функция принимает значение 0, то есть $h(\tilde{b}) = h(\tilde{a}) = 0$;

2) на наборе $\bar{\tilde{b}} = (\bar{b}_1, ..., \bar{b}_r)$ и на всех наборах $\tilde{c} = (c_1, ..., c_r)$, таких, что расстояние Хэмминга между ними не более k, т.е.

$$\rho(\tilde{c}, \bar{\tilde{b}}) = \sum_{i=1}^{2k+1} |c_i - \bar{b}_i| \leq k,$$

функция принимает значение 1, то есть $h(\bar{\tilde{b}}) = h(\tilde{c}) = 1$.

Для функций из множества H_r множество наборов переменных можно представить в виде двух шаров радиуса k, центром одного из них является характеристический набор $\tilde{b} = (b_1, ..., b_r)$, на котором функция $h(x_1, ..., x_r)$ принимает значение 0, а все остальные нулевые наборы функции, отличные от $\tilde{b}$ не более чем на k компонент, лежат внутри этого шара. Центром другого шара является набор $\bar{\tilde{b}} = (\bar{b}_1, ..., \bar{b}_r)$, на котором функция $h(x_1, ..., x_r)$ принимает значение 1, а все остальные единичные наборы функции, отличные от $\bar{\tilde{b}}$ не более чем на k компонент, лежат внутри этого шара. Расстояние между характеристическим наборами функции $h(x_1, ..., x_r)$ равно r, поэтому расстояние между шарами $\rho \geq 2$.

Множество H_r содержит 2^r функций.

Задача данной работы состоит в том, чтобы показать, что наличие хотя бы одной функции из множества H_r в базисе позволяет повысить ненадежность схем, реализующих булевы фукциии в указанном базисе.

Основной результат работы содержит теорема 1.

Теорема 1. *Пусть m — наибольшее число входов элементов в полном конечном базисе B, содержащем хотя бы одну функцию $h(x_1, ..., x_r)$ множества H_r ($m \geq 3$), существенно зависящую от $2k + 1 \leq r$ переменных, тогда любую булеву функцию $f(\tilde{x})$ в базисе B при $\varepsilon \leq \frac{1}{2 \cdot 24^2 c^3 m^2}$ можно реализовать схемой S, ненадежность которой $P(S) \leq a\varepsilon^{k+1} + \varepsilon^{k+2}$, где $a = C_r^{k+1} + 1, k = 1, 2, ..., c = rC_r^{[r/2]}$.*

Таким образом, из теоремы 1 следует, что при инверсных неисправностях на входах элементов наличие хотя бы одной функции $h(x_1, ..., x_r)$ множества H_r в полном конечном базисе B позволяет реализовать все булевы функции схемами с ненадежностью не более $a\varepsilon^{k+1}+\varepsilon^{k+2}$ при $\varepsilon \leq \frac{1}{2\cdot 24^2 c^3 m^2}$, где $a = C_r^{k+1}+1, k = 1, 2, ..., c = rC_r^{[r/2]}$, m — наибольшее число входов элементов в полном конечном базисе B ($m \geq 3$).

Рассмотрим пример.

Пусть базис B^* содержит функции $x_1\&x_2$, $x_1 \vee x_2$, $\bar{x}_1$ и хотя бы одну функцию множества H_r ($m \geq 3$), тогда для него можно доказать теоремы 2 и 3.

Теорема 2. *Пусть m — наибольшее число входов элементов в полном конечном базисе B^*, тогда любую булеву функцию $f(\tilde{x})$ в базисе B^* при $\varepsilon \leq \frac{1}{2\cdot 24^2 c^3 m^2}$ можно реализовать схемой S, ненадежность которой $P(S) \leq a\varepsilon^{k+1} + \varepsilon^{k+2}$, где $a = C_r^{k+1} + 1, k = 1, 2, ..., c = rC_r^{[r/2]}$.*

Пусть $K^*(n)$ — множество, содержащее функции $x_i, \bar{x}_i$ ($i = \overline{1, n}$) и константы 0, 1. Очевидно, число функций во множестве $K^*(n)$ равно $2n+2$ и мало по сравнению с общим числом 2^{2^n} булевых функций от n переменных.

В базисе B^* справедлива теорема 3.

Теорема 3. *Пусть $\varepsilon \in (0; \frac{1}{2a}]$, $f(\tilde{x})$ — булева функция, $f \notin K^*(n)$, и S — любая схема в базисе B^*, реализующая f. Тогда $P(S) \geq a\varepsilon^{k+1}(1-\varepsilon)^k$, где $a = C_r^{k+1} + 1, k = 1, 2, ...$*

Таким образом, из теорем 2 и 3 следует, что в базисе B^* произвольную булеву функцию, кроме функций $x_i, \bar{x}_i$ ($i = \overline{1, n}$) и констант 0, 1, можно реализовать схемой с ненадежностью асимптотически (при $\varepsilon \to 0$) равной $a\varepsilon^{k+1}$, где $a = C_r^{k+1} + 1, k = 1, 2, ...$

Полученный в базисе B^* результат можно сравнить с результатом, полученным в базисе $\{x_1\&x_2, x_1 \vee x_2, \bar{x}_1\}$. В базисе $\{x_1\&x_2, x_1 \vee x_2, \bar{x}_1\}$ функции x_1, x_2, ..., x_n можно реализовать абсолютно надежно, функции $\bar{x}_1$, $\bar{x}_2$, ..., $\bar{x}_n$ можно реализовать схемами с ненадежностью ε, константы 0 и 1 — с ненадежностью ε^2, а все остальные булевы функции — асимптотически наилучшими по надежности схемами, функционирующими с ненадежностью, асимптотически равной 2ε при $\varepsilon \to 0$ [2].

Таким образом, действительно, наличие хотя бы одной функции из рассматриваемого множества в базисе позволяет повысить надежность схем, реализующих булевы функции.

Список литературы

1. Чугунова В. В. Об одном множестве функций // Известия высших учебных заведений. Поволжский регион. Физико-математические науки. — 2009. — № 2 (10). — С. 2–13.

2. Алехина М. А., Чугунова В. В. Об асимптотически наилучших по надежности схемах в базисе $\{\&, \vee, \bar{}\}$ при инверсных неисправностях на входах элементов // Дискретный анализ и исследование операций. Сер. 1. — 2006. — Т. 13. № 4. — С. 3–17.

МНОГОПАРАМЕТРИЧЕСКАЯ КЛАСТЕРИЗАЦИЯ ДИСКРЕТНЫХ СТОХАСТИЧЕСКИХ ПРОЦЕССОВ ПО ЗАДАННЫМ НАЧАЛЬНЫМ КЛАСТЕРНЫМ ЦЕНТРАМ

С. В. Шалагин, А. Р. Нурутдинова (Казань)

Предложена методика кластеризации дискретных стохастических процессов класса марковских по множеству характеризующих признаков.

Пусть задано множество из N объектов — X, каждый из которых характеризуют m признаков. Для анализа X определена таблица объект-признак, содержащая $N + k$ строк и m столбцов [1, 2]. В данную таблицу, под номерами $1 - k$, введены k объектов (по количеству кластеров) — $X^{(1)}, ..., X^{(k)}$. Векторы значений признаков, характеризующие $X^{(1)}, ..., X^{(k)}$ позволяют определить данные объекты как "идеальные". При использовании дивизивного метода кластеризации "k-средних" [1, 3, 4] множество X разбивается на априори заданное количество кластеров k. В i-й кластер помещаются объекты, наиболее близкие к $X^{(i)}, i = \overline{1,\ k}$, по Евклидовой метрике. Пусть для X справедливо

Определение. *При кластеризации множества X на подмножества $G_1, ..., G_k : \sum_{i=1}^{k} G_i = N + k, G_i \cap G_j = \emptyset, i, j = \overline{1,\ k}, i \neq j$, при использовании дивизивного метода для заданного пространства признаков с начальными кластерными центрами $X^{(1)}, ..., X^{(k)}$,*

$$\forall i = \overline{1,\ k}, \exists X_i : D_E(X_j, ..., X^i) < \min D_E(X^l, X^{(i)}), (l = \overline{1,\ k})\&(l \neq i), \quad (1)$$

Тогда имеет место

Утверждение. *Если для X справедливо условие* (1), *то* $X^i \in G_i, i = \overline{1,\ k}$.

Справедливость данного утверждения следует из того, что для метода "k-средних" производится оптимизация разбиений на кластеры исходя из минимизации внутрикластерных и максимизации межкластерных расстояний [1, 3, 4]. Если предположить, что $X^{(l)}$ и $X^{(i)}$ войдут в один из кластеров, то максимальное внутрикластерное расстояние для него будет, согласно определению,не менее чем $minD_E(X^{(l)}, ..., X^{(i)})$, $(l = \overline{1,\ k})\&(l \neq i)$. Что не возможно для заданного множества X.

Кластеризация $(N+k)$ объектов при справедливости условия (1), осуществляется таким образом, что в каждом кластере G_i, $i = \overline{1,\ k}$, существует не менее двух объектов, один из которых — "идеальный" объект $X^{(i)}$. Если из N объектов требуется выделить n, наиболее приближенных к одному из "идеальных" объектов, например к $X^{(1)}$, то предложенная методика включает два этапа. Этап 1 — разделение множества объектов на k кластеров — $G_1, ..., G_k$, $k > 1$. Этап 2 — определение соотношения количества объектов, находящихся в G_1 и в подмножествах $G_2, ..., G_k$. Если $|G_1| > 1$, то объекты, включенные в подмножества $G_2, ..., G_k$, исключаются из дальнейшего рассмотрения, а методика выполняется рекурсивно — из множества объектов G_1 выделяется $n = d$ объектов, наиболее приближенных к $X^{(1)}$. Если $|G_1| < n$, то выделяются $|G_1|$ объектов, а методика выполняется рекурсивно — из множества объектов $G_2 + ... + G_k$ выделяются $d = (n - |G_1|)$ объектов, наиболее приближенных к $X^{(1)}$. Если $|G_1| = d$, то искомое решение найдено.

Замечание 1. Методика справедлива при выполнения условия вида (1).

Замечание 2. При использовании предложенной методики в общем случае возможен отбор f подмножеств, включающих $n_1, ..., n_f$ объектов соответственно, $f < k$, при условии, что $\sum_{j=1}^{f} n_j < N$. Для полученного кластерного решения возможно выполнить коррекцию и визуализацию результатов кластеризации согласно методике [2], определив кластеры как группы и выполнив дискриминантный анализ [3]. Диаграммы рассеивания, построенные для результатов

при использовании полученных линейных дискриминантных функций, позволяют визуально оценить полученные результаты дискриминации [3].

Список литературы

1. Дюран Б., Оделл П. Кластерный анализ. — М.: Статистика, 1977.

2. Захаров В. М., Нурмеев Н. Н., Салимов Ф. И., Соколов С. Ю., Шалагин С. В. Классификация стохастических эргодических матриц методами кластерного и дискриминантного анализа // Исследования по информатике. — 2000. — Вып. 2. — С. 91–106.

3. Ким Дж. О, Мьюллер Ч. У., Клекка У. Р., Олдендерфер М. С., Блэшфилд Р. К. Факторный, дискриминантный и кластерный анализ. — М.: Финансы и статистика, 1989.

4. Жамбю М. Иерархический кластер-анализ и соответствия. — М.: Финансы и статистика, 1988.

О СЛОЖНОСТИ ДИАГНОСТИКИ ПЕРЕПУТЫВАНИЙ В СХЕМАХ ФОРМУЛЬНОГО ТИПА

В. И. Шевченко (Нижний Новгород)

Рассматриваются схемы из функциональных элементов формульного типа [1], то есть схемы, в которых разветвления могут быть только на входах схемы, а к выходу каждого элемента схемы может быть присоединен только один вход только одного элемента. При этом в любой из рассматриваемых схем один или несколько входов некоторых элементов могут быть присоединены неправильно (с не теми входами схемы или выходами не тех элементов как это предписано). Для диагностики (поиска) неправильных присоединений используются деревья решений (условные тесты) [2, 3]. В работе для различных конечных базисов для схем исследуются верхние и нижние оценки минимальной глубины деревьев решений в худшем случае. Данная работа является продолжением работы [4].

Предполагается, что каждая схема имеет хотя бы один вход, хотя бы один функциональный элемент и ровно один выход. Конечное множество булевых функций B будем называть *базисом*, а схему S, в которой каждому элементу сопоставлена функция из B, *схемой в базисе* B. Входы S и выходы ее элементов иногда будем называть вершинами. Входы S иногда будем называть вершинами нулевого

яруса, выходы элементов, все входы которых присоединены только к вершинам нулевого яруса — вершинами первого яруса, выходы элементов, все входы которых присоединены только к вершинам нулевого и первого ярусов — вершинами второго яруса и так далее. Пусть число вершин в S равно N. Занумеруем их от 1 до N, при этом сначала нумеруем вершины нулевого яруса, затем вершины первого яруса и так далее. Пусть n — число входов, а l — число элементов в S, тогда через I_1 обозначим множество номеров вершин, к которым присоединены входы элемента с номером $n+1$, через I_2 — множество номеров вершин, к которым присоединены входы элемента с номером $n+2$, и так далее. Заметим, что, так как S — схема формульного типа, то пересечение любой пары различных множеств I_p и I_q либо пусто, либо является подмножеством множества $\{1,\ldots,n\}$. Если при построении схемы S по формуле имели место неправильные присоединения, то это означает, что изменились некоторые из множеств $I_1,\ldots,I_l$ и мы получили схему формульного типа S', которая, возможно, реализует функцию, отличную от функции, реализуемой S. Обозначим через $H(S)$ множество всех схем, которое содержит схему S и все схемы, которые могут быть получены в результате неправльных присоединений. Никаких других схем $H(S)$ не содержит. Множество различных булевых функций, реализуемых схемами из $H(S)$, обозначим через $F(S)=\{f_1,f_2,\ldots,f_m\}$. Разобъем $H(S)$ на подмножества

$$H_1(S),H_2(S),\ldots,H_m(S)$$

такие, что для $i=1,\ldots,m$ все схемы из $H_i(S)$ реализуют одну и ту же булеву функцию f_i. Для удобства будем предполагать, что $S\in H_1(S)$.

Задача диагностики схемы S: для любой схемы U из $H(S)$ определить к какому из подмножеств $H_i(S)$, $i=1,\ldots,m$, принадлежит U. Для решения этой задачи используются деревья решений (условные тесты).

Дерево решений Y для решения задачи диагностики схемы S представляет собой конечное ориентированное корневое дерево, в котором каждой вершине, не являющейся концевой, приписан двоичный набор из $\{0,1\}^n$, каждой концевой вершине — некоторое число из множества $\{1,\ldots,m\}$. Из каждой вершины, не являющейся концевой, исходят ровно две дуги, которым приписаны числа 0 и 1. Далее, для любой функции $f_i\in F(S)$, реализуемой схемами из $H_i(S)$, найдется полный путь (от корня до концевой вершины) $\gamma=v_1,u_1,\ldots,u_r,v_{r+1}$ такой, что вершине v_{r+1} приписано число i и, если при $q=1,\ldots,r$ вершине v_q приписан набор $\alpha_q\in\{0,1\}^n$, а дуге u_q — число $\delta_q\in\{0,1\}$, то функция f_i — един-

ственная функция в $F(S)$, которая на наборах $\alpha_1, \ldots, \alpha_r$ принимает значения $\delta_1, \ldots, \delta_r$ соответственно. Максимальная длина полного пути называется глубиной дерева решений Y и обозначается через $h(Y)$. Величина $d(S) = \min h(Y)$, где минимум берется по всем деревьям решений для диагностики S, называется *минимальной глубиной деревьев решений для диагностики схемы* S. Обозначим через $d_B(N) = \max d(S)$, где максимум берется по всем схемам в базисе B, число вершин в которых не провосходит N. Через $\tau(B)$ будем обозначать максимальное число переменных у функций из B.

Теорема. *а) Если базис B содержит только конъюнкции и, возможно, константы, или только дизъюнкции и, возможно, константы, или только линейные булевы функции и при этом $\tau(B) \geq 2$, то для $N \geq 2$ справедливы неравенства*:

$$N - \lceil (N-1)/\tau \rceil - 1 \leq d_B(N) \leq N - \lceil (N-1)/\tau \rceil.$$

б) Если базис B содержит только монотонные булевы функции и при этом хотя бы одну функцию, отличную от конъюнкции и константы, хотя бы одну функцию, отличную от дизъюнкции и константы, и $2 \leq \tau(B) \leq 3$, то для $N \geq 2$ имеют место неравенства:

$$2^{\lfloor (N-2)/6 \rfloor - 1} \leq d_B(N) \leq \binom{r+1}{\lceil r/2 \rceil + 1}, \quad r = N - \lceil (N-1)/3 \rceil.$$

в) Если базис B содержит немонотонную булеву функцию, нелинейную булеву функцию и $2 \leq \tau(B) \leq 3$, то для $N \geq 2$ имеют место неравенства:

$$2^{\lfloor (N-2)/3 \rfloor - 1} \leq d_B(N) \leq 2^{N - \lceil (N-1)/3 \rceil}.$$

Список литературы

1. Лупанов О. Б. Асимптотические оценки сложности управляющих систем. — М.: Изд-во МГУ, 1984.

2. Мошков М. Ю. Деревья решений. Теория и приложения. — Нижний Новгород: Изд-во ННГУ, 1994.

3. Чегис И. А., Яблонский С. В. Логические способы контроля работы электрических схем // Тр. Матем. ин-та АН СССР. — 1958. — Т. 51. — С. 270–360.

4. Шевченко В. И. О сложности тестирования перепутываний в схемах // Материалы XVI Междунароной школы-семинара "Синтез и сложность управляющих систем" (Санкт-Петербург, 2006 г.). — М.: Изд-во мех-мат ф-та МГУ, 2006. — С. 131–135.

О СТРУКТУРЕ ЛУЧШИХ ДООПРЕДЕЛЕНИЙ

Л. А. Шоломов (Москва)

Задан алфавит $A_0 = \{a_0, a_1, \ldots, a_{m-1}\}$ *основных символов*. Пусть $M = \{0, 1, \ldots, m-1\}$ и каждому (непустому) $T \subseteq M$ сопоставлен символ a_T. Символы алфавита $A = \{a_T, T \subseteq M\}$ и составленные из них последовательности будем называть *недоопределенными*. *Доопределением* символа $a_T \in A$ считается всякий основной символ a_i, $i \in T$, а доопределением последовательности в алфавите A — всякая последовательность, полученная из нее заменой всех символов некоторыми доопределениями.

Пусть $\mathbf{x} = a_{T_1} \ldots a_{T_n}$ — недоопределенная последовательность и $\dot{\mathbf{x}} = a_{i_1} \ldots a_{i_n}$ ее доопределение. Обозначим через u_{Ti} число появлений пары (a_T, a_i) среди (a_{T_s}, a_{i_s}), $s = 1, \ldots, n$. Структуру доопределения $\dot{\mathbf{x}}$ последовательности $\mathbf{x}$ будем характеризовать матрицей $R(\mathbf{x}, \dot{\mathbf{x}}) = \|r_{Ti}\|$ частот $r_{Ti} = u_{Ti}/n$.

Обозначим через $K(\dot{\mathbf{x}})$ колмогоровскую сложность (относительно некоторого оптимального алгоритма) [1] доопределения $\dot{\mathbf{x}}$. Под колмогоровской сложностью $K(\mathbf{x})$ недоопределенной последовательности $\mathbf{x}$ будем понимать $\min K(\dot{\mathbf{x}})$ по всем ее доопределениям. Доопределение, на котором достигается $K(\mathbf{x})$, назовем *лучшим*.

Для набора $\mathbf{l} = (l_T, T \subseteq M)$, $\sum_T l_T = n$, обозначим через $\mathcal{K}_n(\mathbf{l})$ класс всех недоопределенных последовательностей длины n, в которых символы a_T встречаются l_T раз. Будем рассматривать последовательности растущей длины n с фиксированным набором $P = (p_T, T \subseteq M)$ частот символов. Более точно, будем считать, что

$$\frac{l_T}{n} \to p_T, \quad T \subseteq M. \tag{$*$}$$

Задавшись набором $Q = (q_i, i \in M)$, $q_i \geq 0$, $\sum_i q_i = 1$, введем функцию

$$\mathcal{H}(P, Q) = -\sum_T p_T \log \sum_{i \in T} q_i$$

(логарифмы двоичные) и положим $\mathcal{H}(P) = \min\limits_Q \mathcal{H}(P, Q)$. В "типичной ситуации" величина $\mathcal{H}(P)$ достигается на единственном наборе, который будем обозначать $\hat{Q} = (\hat{q}_i, i \in M)$. Достаточным для единственности является довольно слабое условие, чтобы ранг матрицы, имеющей в качестве строк характеристические векторы множеств T, для которых $p_T > 0$, и строку из единиц, был равен m (число

самих строк может достигать 2^m). Вначале будем считать, что точка минимума единственна (этот случай назовем *невырожденным*), затем обратимся к общему случаю.

Положим $\hat{r}_{Ti} = \dfrac{p_T \hat{q}_i}{\sum_{j \in T} \hat{q}_j}$ и образуем матрицу $\hat{R} = \|\hat{r}_{Ti}\|$. Расстояние между матрицами $R' = \|r'_{Ti}\|$ и $R'' = \|r''_{Ti}\|$ будем измерять величиной $d(R', R'') = \max\limits_{T.i} |r'_{Ti} - r''_{T,i}|$.

Следующая теорема показывает, что лучшие доопределения почти всех последовательностей класса $\mathcal{K}_n(\mathbf{l})$ имеют почти одинаковую структуру.

Теорема 1. *Если выполнены условия* $(*)$ *и имеет место невырожденный случай, то для любого* $\varepsilon > 0$ *доля последовательностей* $\mathbf{x} \in \mathcal{K}_n(\mathbf{l})$*, для которых все лучшие доопределения* $\dot{\mathbf{x}}$ *удовлетворяют условию* $d(R(\mathbf{x}, \dot{\mathbf{x}}), \hat{R}) < \varepsilon$*, стремится к* 1 *при* $n \to \infty$.

Положим

$$K(n, \mathbf{l}) = \max_{\mathbf{x} \in \mathcal{K}_n(\mathbf{l})} K(\mathbf{x}).$$

Имеет место асимптотика $K(n, \mathbf{l}) \sim n\mathcal{H}(P)$ [2].

Рассмотрим метод C двоичного кодирования последовательностей $\mathbf{x} \in \mathcal{K}_n(\mathbf{l})$, позволяющий по коду $C(\mathbf{x})$ последовательности восстановить какое-либо ее доопределение, обозначаемое $\dot{\mathbf{x}}_C$. Метод C считается *асимптотически наилучшим*, если длины кодов для всех $\mathbf{x} \in \mathcal{K}_n(\mathbf{l})$ удовлетворяют оценке $|C(\mathbf{x})| \lesssim K(n, \mathbf{l})$.

Теорема 2. *Если выполнены условия* $(*)$*, имеет место невырожденный случай и кодирование* C *является асимптотически наилучшим для класса* $\mathcal{K}_n(\mathbf{l})$*, то для любого* $\varepsilon > 0$ *доля тех* $\mathbf{x} \in \mathcal{K}_n(\mathbf{l})$*, для которых* $d(R(\mathbf{x}, \dot{\mathbf{x}}_C), \hat{R}) < \varepsilon$*, стремится к* 1 *при* $n \to \infty$.

Рассмотрим теперь общий случай, когда множество $\hat{\mathcal{Q}}$ точек минимума функции $\mathcal{H}(P, Q)$ не обязательно одноэлементно. Для каждого $\hat{Q} \in \hat{\mathcal{Q}}$ образуем матрицу $\hat{R} = \|\hat{r}_T i\|$ тем же способом, что и выше, и множество всех полученных матриц $\hat{R}$ обозначим через $\hat{\mathcal{R}}$. Это множество выпукло и замкнуто. Расстояние от матрицы $R = \|r_{Ti}\|$ до множества $\hat{\mathcal{R}}$ будем измерять величиной $d(R, \hat{\mathcal{R}}) = \min\limits_{\hat{R} \in \hat{\mathcal{R}}} d(R, \hat{R})$.

Теорема 3. *Пусть выполнены условия* $(*)$*. Тогда*

1) *для любого метода кодирования* C*, асимптотически наилучшего для класса* $\mathcal{K}_n(\mathbf{l})$*, и любого* $\varepsilon > 0$ *доля тех* $\mathbf{x} \in \mathcal{K}_n(\mathbf{l})$*, для которых* $d(R(\mathbf{x}, \dot{\mathbf{x}}_C), \hat{\mathcal{R}}) < \varepsilon$*, стремится к* 1 *при* $n \to \infty$*;*

2) *для любой матрицы* $\hat{R} \in \hat{\mathcal{R}}$ *существует метод кодирования* C, *асимптотически наилучший для класса* $\mathcal{K}_n(\mathbf{l})$, *такой что для любого* $\varepsilon > 0$ *и всех* $\mathbf{x} \in \mathcal{K}_n(\mathbf{l})$ *выполнено* $d(R(\mathbf{x}, \dot{\mathbf{x}}_C), \hat{R}) < \varepsilon$.

Отметим, что в вырожденном случае, когда точка минимума неединственна, можно построить асимптотически наилучшее кодирование C, при котором матрицы $R(\mathbf{x}, \dot{\mathbf{x}}_C)$ концентрируются вокруг нескольких матриц из $\hat{\mathcal{R}}$ и, следовательно, доопределения $\dot{\mathbf{x}}_C$, связанные с методом C, будут иметь существенно различную структуру.

Полученные результаты допускают модификацию применительно к реализации систем $F(\tilde{x}) = (f_1(\tilde{x}), \ldots, f_k(\tilde{x}))$, $\tilde{x} = (x_1, \ldots, x_n)$, частичных булевых функций (считаем k фиксированным, n — растущим). Систему F будем характеризовать параметрами $l_{\tilde{\alpha}}$, $\tilde{\alpha} \in \{0, 1, *\}^k$, где $*$ означает неопределенное значение, а $l_{\tilde{\alpha}}$ — число наборов $\tilde{x}$, на которых $F(\tilde{x}) = \tilde{\alpha}$. Введем класс $\mathcal{F}_n(\mathbf{l})$ систем F с набором параметров $\mathbf{l} = (l_{\tilde{\alpha}},\ \tilde{\alpha} \in \{0, 1, *\}^k)$. Система F может быть описана в терминах недоопределенных последовательностей длины 2^n, если занумеровать наборы $\tilde{\sigma} \in \{0, 1\}^k$ символами a_i, а каждому $\tilde{\alpha} \in \{0, 1, *\}^k$ сопоставить символ a_T, где T — множество номеров доопределений $\tilde{\sigma}$ набора $\tilde{\alpha}$. Условию $(*)$ соответствует $l_{\tilde{\alpha}} 2^{-n} \to p_{\tilde{\alpha}}$.

Рассматривается реализация систем F схемами в произвольном конечном базисе и лучшим считается доопределение, реализуемое минимальной схемой. Справедливы аналоги теорем 1 и 2, утверждающие, что в невырожденном случае лучшие доопределения почти всех систем из $\mathcal{F}_n(\mathbf{l})$ имеют почти одинаковую структуру, и то же справедливо для доопределений, возникающих при асимптотически наилучших для $\mathcal{F}_n(\mathbf{l})$ методах синтеза.

Работа выполнена при финансовой поддержке ОНИТ РАН по программе фундаментальных исследований.

Список литературы

1. Колмогоров А. Н. Алгоритм, информация, сложность. — М.: Знание, 1991.

2. Шоломов Л. А. Сжатие частично определенной информации // Нелинейная динамика и управление. Вып. 4. — М.: Физматлит, 2004. — С. 385–399.

О СЛОЖНОСТИ ПРЕДИКАТНЫХ СХЕМ В БАЗИСАХ ИЗ ЭЛЕМЕНТОВ С НЕ БОЛЕЕ ЧЕМ ТРЕМЯ ПОЛЮСАМИ

М. С. Шуплецов (Москва)

Задача синтеза [2, 6] для модели схем из предикатных элементов ранее исследовалась в работах [4] и [5], в которых для достаточно широкого класса базисов была получена асимптотика функции Шеннона для сложности предикатных схем, а также оценки высокой степени точности [3] для более узкого класса базисов. В данной работе вводится некоторое уточнение рассматриваемой модели, которое позволяет получить асимптотику функции Шеннона для произвольного предикатно полного базиса, который содержит предикатные элементы с не более чем тремя полюсами.

Предикатная схема представляет собой двудольный граф, у которого все вершины одной доли помечены символами базисных предикатных элементов, а вершины другой доли — символами внутренних и входных переменных. Функционирование предикатного элемента с k полюсами задается его характеристической функцией от k переменных, связанных с этими полюсами, и определяется тем, что элемент находится в допустимом состоянии, если данная функция равна 1. Схема находится в допустимом состоянии на некотором наборе значений входных переменных тогда и только тогда, когда существует набор значений внутренних переменных такой, что все предикатные элементы, из которых построена схема, находятся в допустимых состояниях. Соответствующий набор входных переменных схемы будем называть допустимым.

Рассмотрим следующую модификацию модели схем из предикатных элементов. Будем считать, что каждая вершина второй доли, помеченная символом внутренней переменной y, отвечает коммутационному узлу специального вида, который содержит четыре вершины, отвечающие функциям y, $\overline{y}$, 0 и 1, соответственно. При этом каждое ребро дополнительно помечается, чтобы указать к какой из четырех вершин коммутационного узла оно присоединено. Таким образом, каждая внутренняя переменная предикатной схемы может входить в характеристическую функцию базисного предиката с отрицанием или забиваться константой.

Подмножество M, состоящее из r, $r \geqslant 2$, переменных предиката $\pi(x_1, \ldots, x_n)$, будем называть его обобщенной существенной переменной (ОП), если существует такой набор β значений остальных переменных предиката, подстановка которого вместо указанных переменных даст предикат, отличный от тождественно истинного предиката и допустимый на двух противоположных наборах α и $\overline{\alpha}$ зна-

чений переменных из M. При этом набор β будем называть *определяющим*, а наборы α и $\overline{\alpha}$ — *основными* наборами ОП M предиката π. Введенное понятие является распространением аналогичного понятия из работы [1] на модель схем из предикатных элементов.

Предикат $\pi(x_1, \ldots, x_n)$ будем называть *блочным*, если его характеристическая функция χ_π может быть представлена в следующем виде: $\chi_\pi(x_1, \ldots, x_n) = \chi_{\pi_1}(x_{i_1}, \ldots, x_{i_{s_1}}) \cdot \ldots \cdot \chi_{\pi_k}(x_{i_{s_{k-1}+1}}, \ldots, x_{i_n})$, где $k \geqslant 2$, π_i, $i = \overline{1,k}$ — некоторые предикаты, существенно зависящие от всех своих переменных, а $x_{i_1}, \ldots, x_{i_n}$ — некоторая перестановка переменных предиката π. При этом предикат π_i, $i = \overline{1,k}$ будем называть *блоком* предиката π. Линейным будем называть предикат (блок) с линейной характеристической функцией, которая существенно зависит от двух и более переменных.

Как и в работе [5] рассмотрим произвольный базис $\mathfrak{B} = \{\pi_i\}_{i=1}^r$, где каждому предикату π_i, $i = \overline{1,r}$ с k_i полюсами, h_i, $h_i \leqslant k_i$, нелинейными блоками и s_i, $s_i \leqslant k_i - h_i$, линейными блоками сопоставлено положительное число L_i, которое характеризует вес этого предиката. Пусть m_i^j — число минимальных по включению ОП предиката π_i, $i = \overline{1,r}$, содержащих переменную x_j. Тогда приведенным весом ρ_i предиката $\pi_i, \pi_i \in \mathfrak{B}$, назовем следующую величину:

$$\rho_i = \min_{j:\, m_i^j \geqslant h_i + 2s_i} \frac{L_i}{m_i^j - h_i - 2s_i + 1}.$$

В случае, когда для любого j условие не выполняется, будем считать, что приведенный вес такого предиката равен бесконечности. Отметим, что любой полный базис содержит не менее одного базисного предиката для которого приведенный вес отличен от бесконечности. Величину $\rho_{\mathfrak{B}} = \min_{\pi_i \in \mathfrak{B}} \rho_i$ будем называть минимальным приведенным весом базиса $\mathfrak{B}$.

Пусть $\mathcal{U}_{\mathfrak{B}}$ — класс предикатных схем, построенных в базисе $\mathfrak{B}$, а $\Pi_2(n)$ — множество всех булевских предикатов от n переменных. Под сложностью $L_{\mathfrak{B}}(\Sigma)$ предикатной схемы Σ, $\Sigma \in \mathcal{U}_{\mathfrak{B}}$, понимается сумма весов её предикатов, а под сложностью $L_{\mathfrak{B}}(\phi)$ предиката ϕ — минимальная из сложностей реализующих его схем. Введем обычным образом функцию Шеннона $L_{\mathfrak{B}}(n) = \max_{\phi \in \Pi_2(n)} L_{\mathfrak{B}}(\phi)$ для класса $\mathcal{U}_{\mathfrak{B}}$ предикатных схем в базисе $\mathfrak{B}$ относительно функционала сложности L.

Теорема. *Если $\mathfrak{B}$ — произвольный предикатно-полный базис, сожержащий предикат с не более чем тремя полюсами, то для*

функции Шеннона $L_{\mathfrak{B}}(n)$ выполняется следующее асимптотическое равенство:

$$L_{\mathfrak{B}}(n) \sim \rho_{\mathfrak{B}} \frac{2^n}{n}.$$

Работа выполнена при финансовой поддержке РФФИ (грант 09-01-00817-а).

Список литературы

1. Долгополова А. В. Задача синтеза и проблемы полноты для одного класса схем из функциональных элементов, связанных с электронными схемами // Диссертация на соискание ученой степени кандидата физико-математических наук. — М., 2003.

2. Лупанов О. Б. Асимптотические оценки сложности управляющих систем. — М.: Изд-во МГУ, 1984.

3. Ложкин С. А. Оценки высокой степени точности для сложности управляющих систем из некоторых классов // Математические вопросы кибернетики. Вып. 6. — М.: Наука. Физматлит, 1996. — С. 189–214.

4. Шуплецов М. С. Асимптотика функции Шеннона в некоторых базисах с элементами блочного типа // Материалы XVII Международной школы-семинара "Синтез и сложность управляющих систем" имени академика О. Б. Лупанова (Новосибирск, 27 октября – 1 ноября 2008 г.). — Новосибирск: Изд-во института математики, 2008. — С. 196–201.

5. Шуплецов М. С. Оценки высокой степени точности для сложности предикатных схем в некоторых базисах // Ученые записки Казанского университета. Сер. Физико-математические науки. — 2009. — Т. 151, кн. 2. — С. 173–184.

6. Shannon C. E. The synthethis of two-terminal switching circuits // Bell Syst. Techn. J. — 1949. — V. 28, № 1. — P. 59–98.

Секция «Функциональные системы»

КРИТЕРИИ ПОЛНОТЫ ДЛЯ КЛАССОВ РАСШИРЕННОЙ СУПЕРПОЗИЦИИ

Я. В. Акулов (Москва)

Э. Пост получил полное описание семейства замкнутых (относительно операции суперпозиции) классов функций двузначной логики [1, 2] (см. также [3, 4]). Как показал Пост, мощность этого множества является счетной. Напротив, известно [5], что множество всех замкнутых классов k-значной логики при $k \geq 3$ имеет континуальную мощность. В связи с этим исследование множества замкнутых классов многозначной логики сопряжено со значительными трудностями. В ряде работ рассматриваются другие операции замыкания, позволяющие получить более "просто" устроенное множество замкнутых классов. Обзор некоторых результатов, полученных в этом направлении, см., например, в [6].

В данной работе рассматривается задача о реализации булевых функций формулами специального вида. Вводится понятие операции расширенной суперпозиции и рассматриваются системы булевых функций, получаемые путем пополнения замкнутых классов с помощью этой операции. Получены критерии полноты для рассматриваемых функциональных систем. Необходимые определния можно найти в [7].

Пусть F — множество булевых функций, содержащее все селекторные функции и замкнутое относительно операций введения несущественных переменных и переименования переменных. Будем называть такие множества *инвариантными классами*. Равенство функций будем понимать с точностью до несущественных переменных. Поэтому операцию введения несущественных переменных в определении инвариантного класса можно опустить. Обозначим через $\mathcal{F}$ семейство всех инвариантных классов булевых функций. Очевидно, что всякий замкнутый класс булевых функций, содержащий функции, отличные от констант, является инвариантным классом. Необходимо подчеркнуть, что это понятие инвариантного класса отличается от понятия инвариантного класса, введенного С. В. Яблонским [8]. Отметим также, что инвариантный класс в

описанном выше смысле является частным случаем инвариантного класса в терминах, введенных в работе [9].

Пусть $F \in \mathcal{F}$, $\mathfrak{A} \subseteq P_2$. Пару таких множеств $(F, \mathfrak{A})$ будем называть *типом* булевых функций. Определим понятие *формулы над типом* $U = (F, \mathfrak{A})$ индуктивно.

1. Выражение $g(x_{i_1}, x_{i_2}, \ldots, x_{i_n})$, где $g \in F$, $x_{i_1}, \ldots, x_{i_n}$ — символы переменных, $n \geq 1$, является формулой над U. Такие формулы будем называть *тривиальными* формулами над U.

2. Пусть $\Phi_1, \Phi_2, \ldots, \Phi_n$ — формулы над U, $n \geq 1$, а $f \in \mathfrak{A}$. Выражение Φ вида $f(\Phi_1, \Phi_2, \ldots, \Phi_n)$ является формулой над U. Будем называть $\Phi_1, \ldots, \Phi_n$ подформулами формулы Φ. Формулу Φ и все подформулы формул $\Phi_1, \ldots, \Phi_n$ будем также называть подформулами формулы Φ.

Формулу Φ, содержащую символы переменных $x_1, \ldots, x_n$ и не содержащую других символов переменных, будем обозначать через $\Phi(x_1, \ldots, x_n)$.

Заметим, что всякая формула над типом $(F, \mathfrak{A})$ является формулой над множеством $F \cup \mathfrak{A}$ и поэтому реализует некоторую булеву функцию. Способ реализации булевых функций формулами указанного вида будем называть операцией *расширенной суперпозиции*.

Пусть $\mathfrak{A} \subseteq P_2$, $F \in \mathcal{F}$. *Пополнением* системы $\mathfrak{A}$ относительно класса F назовем множество всех булевых функций, реализуемых нетривиальными формулами над типом $(F, \mathfrak{A})$ (обозначение $[\mathfrak{A}]_F$). Отметим, что, если F состоит только из селекторных функций, то $[\mathfrak{A}]_F = [\mathfrak{A}]$. Будем называть тип $(F, \mathfrak{A})$ *полным* (в P_2), если $[\mathfrak{A}]_F = P_2$.

Имеет место следующая

Теорема. *Для любого множества $\mathfrak{A}$ булевых функций выполняется по крайней мере одно из следующих утверждений.*

1. *Существует конечная система множеств булевых функций $B(\mathfrak{A}) = \{\mathfrak{B}_1, \ldots, \mathfrak{B}_n\}, n \geq 1$, такая, что для произвольного инвариантного класса F тип $(F, \mathfrak{A})$ является полным тогда и только тогда, когда $F \cap \mathfrak{B}_i \neq \varnothing$ для всех $1 \leq i \leq n$.*

2. *Существует счетная система множеств булевых функций $C(\mathfrak{A}) = \{\mathfrak{C}_1, \mathfrak{C}_2, \ldots\}$, такая, что для произвольного инвариантного класса F тип $(F, \mathfrak{A})$ является полным тогда и только тогда, когда $F \cap \mathfrak{C}_i \neq \varnothing$ для всех $i \geq 1$.*

Следует отметить, что для каждого замкнутого класса булевых функций A можно привести примеры таких систем. Отметим также, что для множеств булевых функций $\mathfrak{A}_1$ и $\mathfrak{A}_2$ указанные системы множеств совпадают, если $[\mathfrak{A}_1] = [\mathfrak{A}_2]$.

В качестве примера рассмотрим случай $[\mathfrak{A}] = L$ (где L — мно-

жество всех линейных булевых функций). Пусть $\mathfrak{C}_i$ — все булевы функции ранга $i-1$, т. е. такие функции, что мономы максимальной степени в их полиномах Жегалкина имеют степень $i-1$, $i=1,2,\ldots$. Искомой системой множеств для этого случая является система $\{\mathfrak{C}_i\}, i \geq 1$. Получаем следующий критерий полноты: для инвариантного класса F и системы булевых функций $\mathfrak{A}$, такой что $[\mathfrak{A}] = L$, равенство $[\mathfrak{A}]_F = P_2$ выполняется тогда и только тогда, когда для любого $i \geq 0$ класс F содержит некоторую функцию ранга i.

Работа выполнена при финансовой поддержке РФФИ (проект 08–01–00863), программы поддержки ведущих научных школ РФ (проект НШ–4437.2010.1) и программы фундаментальных исследований ОМН РАН «Алгебраические и комбинаторные методы математической кибернетики и информационные системы нового поколения».

Список литературы

1. Post E. L. Introduction to a general theory of elementary propositions // Amer. J. Math. — 1921. — V. 43, № 3. — P. 163–185.

2. Post E. L. Two-valued iterative systems of mathematical logic // Annals of Math. Studies. — Princeton—London: Princeton Univ. Press, 1941. — 5. — P. 122.

3. Угольников А. Б. О замкнутых классах Поста // Известия ВУЗов. Математика. — 1988. — № 7 (314). — С. 79–88.

4. Яблонский С. В., Гаврилов Г. П., Кудрявцев В. Б. Функции алгебры логики и классы Поста. — М.: Наука, 1966.

5. Янов Ю. И., Мучник А. А. О существовании k-значных замкнутых классов, не имеющих конечного базиса // Докл. АН СССР. — 1959. — Т. 127, № 1. — С. 44–46.

6. Тарасова О. С. Классы функций трехзначной логики, замкнутые относительно операций суперпозиции и перестановок // Математические вопросы кибернетики. Вып. 13. — 2004. — С. 59–112.

7. Яблонский С. В. Введение в дискретную математику. — М.: Высшая школа, 2006.

8. Яблонский С. В. Об одном семействе классов функций алгебры логики, допускающих простую схемную реализацию // Труды III Всесоюзного математического съезда. Т. 2. — 1956. — С. 149.

9. Кузнецов Ю. В. О классах булевых функций, инвариантых относительно отождествления переменных // Докл. АН СССР. — 1986. — Т. 290, № 4. — С. 780–785.

ОПТИМИЗАЦИЯ СИСТЕМЫ МАССОВОГО ОБСЛУЖИВАНИЯ С КОНЕЧНЫМИ ИСТОЧНИКАМИ ТРЕБОВАНИЙ

В. А. Бадоев (Ярославль), А. В. Угланов (Санкт-Петербург)

Постановка задачи

Рассматривается система $G_k/D_k/1/(n_1,\ldots,n_k)$: на обслуживающий прибор поступают $k \geq 2$ независимых потоков требований, причем i-й поток формируется конечным источником объема n_i так, что каждое требование поступает (независимо от других) после пребывания в источнике случайное время с функцией распределения $F = 1 - e^{-\lambda_i t}$ $(\lambda_i > 0)$. Ориентированный на i-й поток прибор "разогревается" в течение времени, равном t_i, затем мгновенно обслуживает (т.е. возвращает в i-й источник) все требования, затем "остывает" в течение времени, равном s_i, после чего снова готов к работе (т. е. к ориентации на тот или иной поток). Считается, что $t_i + s_i > 0$ для всех $i = 1,\ldots,k$. Управлением (стохастическим стационарным) назовем вектор $(p_1,\ldots,p_k)$, где $p_i \geq 0$, $\sum p_i = 1$. Управление определяет дисциплину обслуживания требований, т. е. работу системы массового обслуживания (СМО), следующим образом: обслуживающий прибор включается в момент $\tau^0 = 0$ и действует непрерывно; если τ^n $(n = 0,1,\ldots)$ есть n-ый по счёту момент готовности прибора, то он (прибор) ориентируется на i-ый поток с вероятностью p_i. Уточним, что ориентация осуществляется вероятностным диспетчером, работа которого не зависит ни от τ^n, ни от состояния СМО, ни от работы диспетчера в прошлом.

Положим $x = x(t) = \{x_i(t)\}$ $(i = 1,\ldots,k; t \in [0,\infty))$, где $x_i(t) = 1 - n_i^{-1} y_i(t)$, где $y_i(t)$ есть число требований i-го потока в момент t ($x_i(t)$ есть мгновенный коэффициент готовности i-го источника). Обозначим через U множество всех управлений и для $u \in U$ положим:

$$R_i = R_i(u) = \lim_{T\to\infty} \frac{1}{T} \int_0^T \mathsf{M} x_i(t)\, dt, \qquad R = R(u) = \min_{1\leq i\leq k} R_i$$

(здесь и далее M есть знак математического ожидания, R_i есть коэффициент готовности i-го источника, R — равномерный коэффициент готовности СМО).

Управление $u^0 \in U$ назовем оптимальным, если $R(u^0) = R^0 = \sup_{u\in U} R(u)$. Задача: найти оптимальное управление.

Замечание. Задача представляет интерес для инженерии (проектирование различных систем технического обслуживания), теории информации (централзованная обработка информационных потоков), военной науки (задача начала исследоваться вторым автором по заказу одного НИИ Минобороны).

Результаты

Везде ниже: $i, j = 1, \ldots, k$; $\tau_i = t_i + s_i$; $\alpha_{i,j} = \tau_i \lambda_j$; $\beta_{i,j} = e^{-\alpha_{i,j}}$.

В работе [1] для случая $\lambda_1 = \ldots = \lambda_k = \lambda$ получен следующий результат (в указанном случае наши обозначения примут вид $\alpha_i = \tau_i \lambda$, $\beta_i = e^{-\alpha_i}$).

Теорема 1. *Оптимальное стационарное управление существует, единственно и определяется равенствами* $p_m = \gamma(z - \beta_m)^{-1}$ $(m = 1, \ldots, k)$, *где* z *есть единственное на интервале* $(1, \infty)$ *решение уравнения* $\sum_{i=1}^{k}(1 - \beta_i)(z - \beta_i)^{-1} = 1$, $\gamma = \left[\sum_{i=1}^{k}(z - \beta_i)^{-1}\right]^{-1}$. *Кроме того,* $R = R_1 = \ldots = R_k = \left[z \sum_{i=1}^{k} \alpha_i (z - \beta_i)^{-1}\right]^{-1}$.

Главной трудностью при доказательстве теоремы было установление равенств

$$R_1 = \ldots = R_k \tag{1}$$

(при оптимальном управлении). На первый взгляд равенства представляются очевидными. Однако очевидность эта — кажущаяся. Дело в том, что СМО, управляемая вероятностным диспетчером, функционирует по довольно сложным законам. В частности, здесь возможны "гироскопические эффекты": увеличение p_m может приводить к уменьшению R_m. Причину этого, впрочем, понять нетрудно. Однако следующий результат уже́ можно отнести к разряду паталогических. Именно, изменим работу вероятностного диспетчера следующим образом: в каждый момент τ_n готовности прибора он (прибор) с вероятностью p_0 "отдыхает" время $\tau_0 > 0$ (так что $\tau_{n+1} = \tau_n + \tau_0$), а с вероятностью $1 - p_0$ функционирует по вышеуказанным правилам (т.е., ориентируется на i-й поток с вероятностью p_i, $\sum_{i=1}^{k} p_i = 1$). Величина R определяется как и выше (конечно, теперь будет $R = R(p_0, p_1, \ldots, p_k)$). Так вот, построен пример, когда $p_0 > q_0$, но $R(p_0, p_1, \ldots, p_k) > R(q_0, p_1, \ldots, p_k)$; другими словами, прибор отдыхает больше, но система функционирует лучше (и это при неизменной приоритетности потоков требований!). Далее, "оче-

видность" равенств (1) заметно уменьшается следующими обстоятельствами.

1. Равенства, вообще говоря, нарушаются, если величины t_i, s_i — случайные (хотя бы даже "абсолютно независимые"); соответствующий пример построен А. В. Углановым уже́ при $k = 2$ (!).

2. Теорема 1 была доказана более двадцати лет назад; при этом "ключевые" равенства (1) доказывались непосредственным анализом уравнений Лагранжа для соответствующей экстремальной задачи. С тех пор и А. В. Углановым, и его учениками предпринимались многочисленные попытки обобщения теоремы (точнее — доказательства равенств (1)) на случай различных λ_i, но безрезультатно. С другой стороны, многочисленные компьютерные эксперименты неизменно показывали, что равенства 1 выполняются.

Теперь нами получен следующий результат (Теорема 2), но сначала приведем необходимую лемму.

Лемма. *Для любого управления и любого j справедливо равенство*

$$R_j = p_j \Big[1 - \textstyle\sum_{i=1}^{k} p_i\,\beta_{i,j}\Big] \Big[\Big(1 - \textstyle\sum_{i\neq j}^{k} p_i\,\beta_{i,j}\Big)\Big(\textstyle\sum_{i=1}^{k} p_i\,\alpha_{i,j}\Big)\Big]^{-1}. \quad (2)$$

Теорема 2. *Существует оптимальное управление $(p_1, \ldots, p_k)$, являющееся решением системы уравнений $R_1 = \ldots = R_k$, $\sum_{i=1}^{k} p_i = 1$, где R_i определяются равенствами* (2).

Замечание. В отличие от вышеуказанного результата работы [1] мы не смогли доказать единственность решения приведеной в теореме 2 системы и, как следствие — единственность оптимального управления.

Работа второго автора выполнена при финансовой поддержке Российского фонда фундаментальных исследований (проект 09-01-00677).

Список литературы

1. Uglanov A. V., Filatova L. Yu. On optimal organization of queueing systems with finite sources of requirements // Seminari di probabilita e statistica matematica. — Cassino (Italy): Univ. di Cassino Press, 1999. — P. 64–95.

ТЕОРИЯ ИМЕНОВАНИЯ С ПУСТЫМ ДЕНОТАТОМ

В. Ю. Винник (Киев)

Явления именования играют в программировании важную роль и во многом определяют саму его сущность. В теории программирования это в явном виде учитывается в композиционном (КП) подходе и его продолжениях [1, 2]. В качестве адекватной модели именования в КП используются именные множества (ИМ). ИМ есть функциональное бинарное отношение между именами и денотатами (значениями), т.е. множество вида $s = \{(v_1, d_1), (v_2, d_2), \ldots\}$, удовлетворяющее принципу однозначности именования: из $(v, d') \in s$ и $(v, d'') \in s$ следует $d' = d''$ (содержательно: имя не может обладать одновременно двумя разными значениями). Наиболее очевидная интерпретация ИМ — множество переменных, с которыми работает программа. В связи со спецификой программирования, чаще всего рассматривают конечные ИМ.

В обширной литературе по КП изучаются различные аспекты ИМ и их модификаций. Представляет интерес описание класса ИМ и его свойств посредством простейших операций над ИМ, а также представление известных сложных операций над ИМ как производных от них. Отметим, что в описании класса объектов через задание свойств простейших операций над ними состоит основная идея методов алгебраической спецификации абстрактных типов данных (АТД) [3]. Таким образом, задача данной работы состоит в построении алгебры и аксиоматической теории АТД ИМ.

Всюду далее считаем, что переменные u, v, w принимают значения в классе имен, переменные d, e — в классе денотатов, а переменные s, t — в классе ИМ. Свободные переменные считаем охваченными неявным квантором всеобщности.

Расширим класс денотатов D, введя объект $\perp$, играющий роль "пустого" денотата: в тех случаях, когда в КП говорят, что имя v не имеет денотата в ИМ s, мы будем говорить, что такое имя имеет денотат $\perp$. Тем самым, операция разыменования, выбирающая из ИМ денотат заданного имени (см. ниже), становится всюду определенной. Допустимость подобного рода доопределений нуждается в обосновании: например, доопределить произвольную частично рекурсивную функцию до общерекурсивной невозможно. В данном случае, однако, "пустой" денотат $\perp$ допустим: его можно устранить из теории ценой введения дополнительных операций вместе с соотношениями, определяющими их свойства; следовательно, теория с пустым денотатом описывает, с точностью до замены обозначений, то же понятие, что и теория с частичной операцией разыменования.

Пустота денотата $\perp$ означает, что

$$\{(u_1, d_1), \ldots, (u_m, d_m)\} = \{(u_1, d_1), \ldots, (u_m, d_m), (v_1, \perp), \ldots, (v_n, \perp)\}$$

при $u_i \neq v_j$. В частности, $\emptyset = \{(u, \perp)\}$ для любого u. В качестве базовой операции над ИМ возьмем операцию именования: $put(u, d, s) = s' \cup \{(u, d)\}$, где $s' = \{(v, e) | (v, e) \in s, v \neq u\}$. Содержательно: операция добавляет к данному ИМ один денотат под заданным именем; если имя уже имеет в ИМ какой-либо денотат, новый денотат его полностью замещает, т. е. операция моделирует свойства разрушающего оператора присваивания; подобным образом, $put(u, \perp, s)$ моделирует стирание именованной переменной из памяти.

Легко видеть, что в алгебре ИМ относительно put имеют место соотношения:

$$d \neq e \Rightarrow put(v, d, s) \neq put(v, e, t),$$
$$put(v, \perp, \emptyset) = \emptyset,$$
$$put(v, d, put(v, e, s)) = put(v, d, s),$$
$$u \neq v \Rightarrow put(u, d, put(v, e, s)) = put(v, e, put(u, d, s)).$$

Эти соотношения выражают соответственно: принцип однозначности именования; определение пустого ИМ как неподвижной точки операций удаления; разрушающую природу присваивания; отсутствие у присваивания побочного эффекта.

Приведенная совокупность соотношений достаточно сильна, чтобы описывать класс конечных ИМ и его свойства. В частности, их можно взять в качестве аксиом прикладной теории первого порядка, язык которой состоит из символов индивидных переменных (разделенных по сортам имен, денотатов и ИМ), функционального символа put арности 3 и $\emptyset$ арности 0, знака равенства и логических знаков. Помимо перечисленных, необходима еще аксиома индукции:

$$(\Phi(\emptyset) \wedge (\forall v, d, s.\ \Phi(s) \Rightarrow \Phi(put(v, d, s)))) \Rightarrow \forall s \Phi(s)$$

(содержательно: класс ИМ состоит из объектов, которые могут быть построены из пустого ИМ с помощью операций именования).

Такая формальная теория очевидно имеет модель — алгебру ИМ при тривиальной интерпретации.

Очевидно, $\forall s, v \exists d, t.\ s = put(v, d, t)$. Более того, согласно аксиоме 1, такой денотат d единственен. Следовательно, можно корректно говорить о двухместной алгебраической операции get, такой, что

$$get(v, put(v, d, s)) = d,$$

и использовать данное соотношение вместо аксиомы 1. Перечисленные аксиомы позволяют доказать ряд теорем, содержательно выражающих важнейшие свойства ИМ:

$$put(v, get(v, s), s) = s,$$
$$u \neq v \Rightarrow get(u, put(v, d, s)) = get(v, s),$$
$$\forall s, v \exists d, t.\ s = put(v, d, t) \wedge put(v, \bot, t) = t,$$
$$s = t \Leftrightarrow \forall v.\ get(v, s) = get(v, t).$$

Предпоследнее утверждение содержательно означает *декомпозируемость* ИМ: всякое ИМ можно разделить на именованный денотат и остаток, полученный его удалением. Последнее утверждение представляет собой поведенческое определение равенства ИМ: два ИМ равны, если они ведут себя одинаково при любых операциях разыменования.

Оказывается возможным обосновать более сильный принцип индукции, согласно которому класс ИМ совпадает с множеством тех ИМ, которые можно построить из пустого ИМ такими операциями именования, которые не удаляют и не замещают денотаты:

$$(\Phi(\emptyset) \wedge (\forall v, d, s.\ get(v, s) = \bot \wedge d \neq \bot \wedge \Phi(s) \Rightarrow \Phi(put(v, d, s)))) \Rightarrow \forall s \Phi(s).$$

Список литературы

1. Никитченко Н. С. Композиционные логики номинативных данных // Проблемы программирования. — 2003. — № 3. — С. 29–40.

2. Редько В. Н. Экзистенциальные основания композиционной парадигмы // Кибернетика и системный анализ. — 2008. — № 2. — С. 3–12.

3. Замулин А. В. Типы данных в языках программирования и базах данных. — Новосибирск: Наука, 1987.

ГЕНЕТИЧЕСКИЙ АЛГОРИТМ ПОИСКА МИНИМАЛЬНЫХ ПОЛИМОМОВ БУЛЕВЫХ ФУНКЦИЙ

С. Ф. Винокуров, А. С. Казимиров (Иркутск)

В работе рассматриваются полиномиальные представления булевых функций. Под сложностью полинома будем понимать количество слагаемых в нем, а под сложностью функции $L(f)$ — наименьшую из сложностей полиномов, представляющих данную функцию.

Задача минимизации заключается в нахождении наименьшего полинома для данной функции. Для 6 переменных известен алгоритм точной минимизации [1]. Данный алгоритм основывается на представлении

$$f(x_1,\ldots,x_n) = \bar{x}_n f_1(x_1,\ldots,x_{n-1}) \oplus$$

$$\oplus f_2(x_1,\ldots,x_{n-1}) \oplus x_n f_3(x_1,\ldots,x_{n-1}) \qquad (*)$$

Слагаемые являются функциями меньшего числа аргументов. Одна из функций выбирается в качестве параметра, а остальные находятся из соотношений:

$$f_1(x_1,\ldots,x_{n-1}) \oplus f_2(x_1,\ldots,x_{n-1}) = f(x_1,\ldots,x_{n-1},0)$$

$$f_2(x_1,\ldots,x_{n-1}) \oplus f_3(x_1,\ldots,x_{n-1}) = f(x_1,\ldots,x_{n-1},1)$$

Таким образом, задача минимизации для функции f сводится к задаче нахождения минимума суммы $L(f_1)+L(f_2)+L(f_3)$. Алгоритм точной минимизации заключается в полном переборе всех вариантов для функции-параметра. При этом предполагается, что задача минимизации для функций $n-1$ переменной либо решена, либо ее решение значительно проще, чем для функции f.

Достаточно предварительно получить библиотеку сложностей и минимальных полиномов функций $n-1$ аргументов для вычисления сложности и нахождения минимального полинома любой функции n аргументов.

Однако при $n = 6$ необходимо составить и хранить библиотеку для функций 5 аргументов. Трудности возникают не только с хранением, но и с использованием библиотеки в процессе минимизации. Для ускорения вычислений необходимо хранить библиотеку сложностей размера 2^{32} байт в оперативной памяти, что является серьезной проблемой. Объемы библиотек можно уменьшить, если хранить не все функции, а только представителей классов по некоторой эквивалентности, сохраняющей сложность полиномов. В [1] описан алгоритм, основанный на использовании N-эквивалентности (расстановка отрицаний над аргументами) на 4-х аргументах. В этом алгоритме необходимо хранить сложность $\sim 4 \cdot 10^7$ функций 5 переменных. Однако более эффективным по времени (но не по используемой памяти) будет библиотека, содержащая сложности ровно половины функций 5 переменных. Тогда для любой функции может быть легко найдена [2] SP-эквивалентная ей, содержащаяся в библиотеке.

Однако этот алгоритм точной минимизации имеет ограничение $n = 6$. Использование разложения $(*)$ при созданных библиотеках

уже при $n = 7$ ведет к необходимости минимизации 2^{64} функций 6 переменных, что проблематично при современном состоянии вычислительной техники. Это ограничение приводит к построению и исследованию класса алгоритмов нахождения приближенно минимальных полиномов. В данной работе рассматривается генетический алгоритм нахождения приближенно минимального полинома булевой функции, который опирается на разложение $(*)$ и построенные библиотеки.

Булевы функции имеют естественный вид для генетических алгоритмов. Особью является вектор функции-параметра f_1. Приспособленность особи определяется как сложность полинома для минимизируемой функции, полученной подстановкой f_1 в разложение $(*)$. Генетический оператор мутации реализован в виде изменения нескольких (не обязательно идущих подряд) бит в векторе особи, а оператор кроссовера — в виде обмена как произвольными частями векторов, так и в виде обмена остаточных по одной из переменных.

Пространство поиска в данной задаче является гладким, что позволяет достаточно эффективно применять генетические алгоритмы.

Утверждение. *При изменении одного бита в функции-параметре число слагаемых в соответствующем полиноме меняется не более, чем на* 3.

Тем не менее, нужно применять дополнительные стратегии для выхода из локальных минимумов.

Данный алгоритм тестировался на случайной выборке и на классе функций, дающем наибольшую сложность при $n \leq 6$. Тестовые запуски при $n = 6$ дали точный минимум для практически всех функций за время, на порядок меньшее времени работы алгоритма точной минимизации. Для $n = 7, 8$ алгоритм дает полиномы, сложность которых близка к теоретическим оценкам.

Работа выполнена при финансовой поддержке РФФИ (проект 09-01-00476-а).

Список литературы

1. Gaidukov A. Algorithm to derive minimum ESOPs for 6-variable function // Proceedings of the 5th International Workshop on Boolean Problems. — Freiberg, Germany, 2002. — P. 141–148.

2. Казимиров А. С. Оценка числа классов LP-эквивалентности булевых функций // Вестник Бурятского университета. Серия 13. Математика и информатика. — 2005. — Вып. 2. — С. 17–22.

О КЛАССАХ ФУНКЦИЙ k-ЗНАЧНОЙ ЛОГИКИ, МОНОТОННЫХ ОТНОСИТЕЛЬНО МНОЖЕСТВ ШИРИНЫ ТРИ

О. С. Дудакова (Москва)

Известно [1], что при $k \leq 7$ все предполные классы в P_k являются конечно-порожденными, а начиная с $k = 8$ существуют предполные классы монотонных функций, не имеющие конечного базиса [2] (см. также [3, 4]); полного описания конечно-порожденных предполных классов монотонных функций к настоящему времени не получено. В работах автора [3–6] приведен критерий конечной порожденности для предполных классов функций, монотонных относительно частично упорядоченных множеств ширины два, а также для некоторых других семейств частично упорядоченных множеств найдены условия существования конечных порождающих систем в соответствующих классах монотонных функций. В данной работе продолжены исследования в этом направлении.

Пусть $\mathcal{P}$ — некоторое частично упорядоченное множество с отношением порядка $\leq$. Пусть $a_1, a_2 \in \mathcal{P}$, элементы a_1 и a_2 несравнимы относительно $\leq$. Элемент $b \in \mathcal{P}$ называется *верхней гранью* элементов a_1, a_2, если выполняются неравенства $b \geq a_1$ и $b \geq a_2$. Верхняя грань b элементов a_1, a_2 называется *минимальной верхней гранью* этих элементов, если ни для какой другой верхней грани x этих элементов не выполняется неравенство $b > x$. Через $|\mathcal{P}|$ будем обозначать число элементов множества $\mathcal{P}$. Положим $w_{\mathcal{P}} = \max |J|$, где максимум берется по всем антицепям J множества $\mathcal{P}$; величину $w_{\mathcal{P}}$ будем называть *шириной* множества $\mathcal{P}$. Через $\mathcal{M}_{\mathcal{P}}$ будем обозначать класс всех функций, монотонных относительно частично упорядоченного множества $\mathcal{P}$.

Обозначим через $\mathbb{A}$ семейство всех частично упорядоченных множеств с наименьшим и наибольшим элементами. Отметим, что класс $\mathcal{M}_{\mathcal{P}}$ является предполным тогда и только тогда, когда $\mathcal{P} \in \mathbb{A}$ (см. [7]). Далее, обозначим через $\mathbb{A}_1$ семейство всех множеств $\mathcal{P} \in \mathbb{A}$, не содержащих шестерки элементов $a_1, a_2, b_1, b_2, c_1, c_2$, где a_1 и a_2 — несравнимые элементы, b_1 и b_2 — минимальные верхние грани элементов a_1 и a_2, а c_1 и c_2 — минимальные верхние грани элементов b_1 и b_2.

Имеют место следующие результаты [3, 4, 6].

Теорема 1. *Пусть $\mathcal{P} \in \mathbb{A}$, $w_{\mathcal{P}} \leq 2$. Класс $\mathcal{M}_{\mathcal{P}}$ является конечно-порожденным тогда и только тогда, когда $\mathcal{P} \in \mathbb{A}_1$.*

Теорема 2. *Пусть $\mathcal{P} \in \mathbb{A}$, $|\mathcal{P}| \leq 9$. Класс $\mathcal{M}_{\mathcal{P}}$ является конечно-порожденным тогда и только тогда, когда $\mathcal{P} \in \mathbb{A}_1$.*

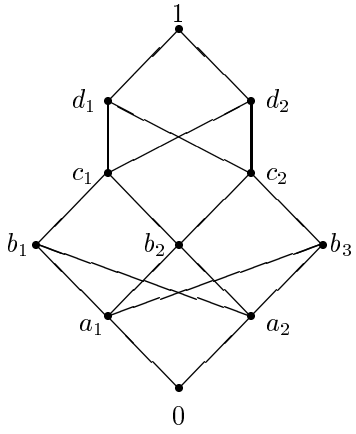


Рис. 1. Множество $\mathcal{Q}$

Следующий пример показывает, что для множеств ширины 3 аналогичный результат в общем случае не имеет места. Пусть $\mathcal{Q}$ — частично упорядоченное множество, изображенное на рис. 1. Легко видеть, что $\mathcal{Q} \in \mathbb{A},\ w_{\mathcal{Q}} = 3$. Кроме того, элементы b_1 и b_3 являются минимальными верхними гранями элементов a_1 и a_2, и элементы d_1 и d_2 являются минимальными верхними гранями элементов b_1 и b_3, поэтому $\mathcal{Q} \notin \mathbb{A}_1$.

Утверждение. *Класс $\mathcal{M}_{\mathcal{Q}}$ является конечно-порожденным.*

Обозначим через $\mathbb{A}^{(3)}$ семейство всех частично упорядоченных множеств из $\mathbb{A}$ ширины 3, которые содержат ровно одну тройку попарно несравнимых элементов. Через $\mathbb{A}_0^{(3)}$ обозначим семейство всех множеств $\mathcal{P} \in \mathbb{A}^{(3)}$, содержащих шестерку элементов a, a', b, b', c, c', для которых выполняются следующие условия:

1) элементы a и a' несравнимы;

2) элементы b и b' — минимальные верхние грани элементов a и a';

3) элементы c и c' — минимальные верхние грани элементов b и b';

4) в $\mathcal{P}$ не существует последовательности элементов $x_0, x_2, \ldots, x_m$, $m \geq 2$, такой что $x_0 = b$, $x_m = b'$, для каждого $i = 1, \ldots, m$ элементы x_i и x_{i-1} сравнимы, для каждого $i = 1, \ldots, m-1$ выполняются неравенства $a, a' < x_i < c, c'$.

Основным результатом данной работы является следующее утверждение.

Теорема 3. *Пусть* $\mathcal{P} \in \mathbb{A}_0^{(3)}$. *Тогда класс* $\mathcal{M}_\mathcal{P}$ *не является конечно-порожденным.*

Работа выполнена при финансовой поддержке РФФИ (проект 08–01–00863), программы поддержки ведущих научных школ РФ (проект НШ–4437.2010.1) и программы фундаментальных исследований ОМН РАН «Алгебраические и комбинаторные методы математической кибернетики и информационные системы нового поколения».

Список литературы

1. Lau D. Bestimmung der Ordnung maximaler Klassen von Funktionen der k-wertigen Logik // Z. math Log. und Grundl. Math. — 1978. — 24. — S. 79–96.

2. Tardos G. A not finitely generated maximal clone of monotone operations // Order. — 1986. — 3. — P. 211–218.

3. Дудакова О. С. О классах функций k-значной логики, монотонных относительно множеств ширины два // Вестн. Моск. ун-та. Серия 1. Математика. Механика. — 2008. — № 1. — С. 31–37.

4. Дудакова О. С. О конечной порожденности предполных классов монотонных функций многозначной логики // Математические вопросы кибернетики. — М.: Физматлит. — 2008. — Вып. 17. — С. 13–104.

5. Дудакова О. С. О конечной порожденности замкнутых классов монотонных функций в P_k // Учен. зап. Казан. ун-та. Серия Физ.-матем. науки. — 2009. — Т. 151, кн. 2. — С. 65–71.

6. Дудакова О. С. О конечной порожденности предполных классов монотонных функций девятизначной логики // Мат-лы XVIII Междунар. школы-семинара "Синтез и сложность управляющих систем" (Пенза, 28 сентября - 3 октября 2009 г.). — М.: Изд-во мех.-матем. ф-та МГУ. — 2009. — С. 38–41.

7. Мартынюк В. В. Исследование некоторых классов в многозначных логиках // Проблемы кибернетики. — М.: Наука. — 1960. — Т. 3. — С. 49–60.

О РАВНОМЕРНОСТИ НЕКОТОРЫХ СИСТЕМ МОНОТОННЫХ ФУНКЦИЙ k-ЗНАЧНОЙ ЛОГИКИ

Д. Ю. Дудоров (Москва)

Рассматривается задача о соотношении глубины и сложности конечных систем функций k-значной логики, монотонных относительно частичных порядков специального вида, $k \geq 3$. Система $\mathfrak{A}$ функций из P_k называется *равномерной*, если существуют такие константы c и d (зависящие от $\mathfrak{A}$), что для любой функции $f \in [\mathfrak{A}]$ выполнено неравенство $D_{\mathfrak{A}}(f) \leq c \log_2 L_{\mathfrak{A}}(f) + d$, где $L_{\mathfrak{A}}(f)$ и $D_{\mathfrak{A}}(f)$, соответственно, есть сложность и глубина функции f в классе формул над $\mathfrak{A}$.

Вопрос о равномерности конечных систем функций был широко исследован ранее. Так, В. М. Храпченко показал [8] (см. также [6]), что любая полная в P_2 система функций равномерна. Аналогичный результат был получен Ф. Спирой [9]. Для конечных полных монотонных систем булевых функций равномерность была доказана И. Венегером [10]. Равномерность произвольных конечных систем булевых функций была показана А. Б. Угольниковым [5]. Им также были приведены примеры неравномерных систем функций в P_k при $k \geq 3$. В работе Р. Ф. Сафина [3] доказано, что любая конечная система функций, монотонных относительно некоторого отношения частичного порядка $\preceq$, порождающая предполный класс в P_k, является равномерной для всех $k \leq 7$, а также в тех случаях, когда частично-упорядоченное множество $(E_k, \preceq)$ является решеткой. Ряд результатов о равномерности систем, порождающих предполные классы функций в P_k, получен в [4].

Множество всех функций k-значной логики обозначим через P_k, $k \geq 2$. Пусть задано отношение частичного порядка $\preceq$ на множестве $E_k = (0, 1, \ldots, k-1)$, $k \geq 2$. Множество всех функций, монотонных относительно частичного порядка $\preceq$, обозначим через $M(\preceq)$. Через $[\mathfrak{A}]$ обозначим замыкание системы $\mathfrak{A}$ относительно операций суперпозиции и введения фиктивных переменных.

Систему $\mathfrak{A}$ функций из P_k назовем *замкнутой относительно операций суперпозиции и введения фиктивной переменной* (*замкнутой*), если она совпадает со своим замыканием относительно указанных операций, т. е. если $[\mathfrak{A}] = \mathfrak{A}$. Очевидно, что множество $M(\preceq)$ является замкнутым. Замкнутые множества функций также называют замкнутыми классами.

Пусть отношение частичного порядка $\preceq$ на множестве E_{2n+2}, $n \geq 2$, задано следующим образом:

1) элемент 0 является наименьшим элементом множества E_{2n+2}, элемент $2n+1$ — наибольшим,

2) элементы $1, 2, \ldots, n$ попарно несравнимы между собой, но каждый из них меньше любого из элементов $n+1, n+2, \ldots, 2n$,

3) элементы $n+1, n+2, \ldots, 2n$ попарно несравнимы между собой.

Обозначим множество E_{2n+2} с вышеописанным частичным порядком на нем через $Y_{2n+2} = (E_{2n+2}, \preceq)$. Все частично-упорядоченные множества такого вида будем называть *базовыми множествами порядка n*. Заметим, что классы монотонных функций относительно частичных порядков указанного вида являются предполными (см. [1]).

Пусть T — замкнутое множество функций из P_k, $k \geq 2$, $0, \ldots, k-1 \in T$ и существует такая функция $\varphi(y, z_0, z_1, \ldots, z_{k-1}) \in T$, что для любой функции $f(y, \tilde{x}) \in T$, $\tilde{x} = (x_1, \ldots, x_p)$, $p \geq 1$ верно равенство

$$f(y, \tilde{x}) = \varphi(y, f(0, \tilde{x}), f(1, \tilde{x}), \ldots, f(k-1, \tilde{x})).$$

Такое T будем называть множеством, удовлетворяющим *условию выразимости*, а функцию φ с указанным выше свойством будем называть *функцией выбора*. Все недостающие определения см. в [7].

Имеет место следующее утверждение.

Теорема. *Пусть $Y_{2n+2} = (E_{2n+2}, \preceq)$ — базовое множество порядка n, $n \geq 2$, а $\mathfrak{A}$ — произвольная конечная система функций из P_{2n+2}, такая, что $[\mathfrak{A}] = M(\preceq)$. Тогда система $\mathfrak{A}$ равномерна.*

Доказательство теоремы опирается на лемму из работы [4] (см. также [2]), согласно которой каждая конечная система функций $k-$значной логики, замыкание которой удовлетворяет условию выразимости, является равномерной. В ходе доказательства теоремы также доказывается ряд лемм, позволяющих определить некоторое множество $R \subset E_{2n+2}^{2n+3}$ для выбранного n, в которое попадают все возможные наборы

$$(y, f(0, \tilde{x}), f(1, \tilde{x}), \ldots, f(2n+1, \tilde{x})),$$

$\tilde{x} = (x_1, x_2, \ldots, x_p)$, $p \geq 1$ для произвольной функции $f \in M(\preceq)$, явно задать на нем частично-определенную монотонную функцию выбора, а затем показать возможность продолжения данной функции до некоторой всюду определенной.

Список литературы

1. Мартынюк В. В. Исследование некоторых классов функций в многозначных логиках // Проблемы кибернетики. Вып.3. — 1960. — С. 49–60.

2. Пратт В. П. Влияние базиса на сложность булевых функций // Кибернет. сборн (новая серия). Вып. 17. — М.: Мир, 1980. — С. 114–123.

3. Сафин Р. Ф. О равномерности систем монотонных функций // Вестн. Моск. ун-та. Серия 1. Матем. Механ. — 2003. — № 2. — С. 15–20.

4. Сафин Р. Ф. О соотношении между глубиной и сложностью формул в предполных классах $k-$значной логики // Матем. вопр. кибернетики. Вып. 13. М.: Физматлит, 2004. — С. 223–278.

5. Угольников А. Б. О глубине и полиномиальной эквивалентности формул для замкнутых классов двузначной логики // Математические заметки. — 1987. — Т. 42, вып. 4. — М.: Наука, 1987. — С. 603–612.

6. Храпченко В. М. О соотношении между сложностью и глубиной формул // Методы дискретного анализа в синтезе управляющих систем. Вып. 32. — Новосибирск, ИМ СО АН СССР, 1978. — С. 76–94.

7. Яблонский С. В. Введение в дискретную математику. — М.: Высшая школа, 2003.

8. Яблонский С. В., Козырев В. П. Математические вопросы кибернетики — информационные материалы Научного совета по комплексной проблеме "Кибернетика" АН СССР. — 1968. — Вып. 19а. — С. 3–15.

9. Spira P. M. On time-hardware complexity tradeoffs for Boolean functions // Proc. 4th Hawai Symposium on System Sciences. — North Hollywood: Western Periodicals Company, 1971. — P. 525–527.

10. Weneger I. Relating monotone formula size and monotone depth of boolean functions // Information Processing Letters. — 1983. — 16 — P. 41–42.

АЛГОРИТМ ПОИСКА БУЛЕВЫХ ФУНКЦИЙ ОТ 6 ПЕРЕМЕННЫХ, СЛОЖНЫХ В КЛАССЕ ПНФ

А. С. Казимиров, С. Ю. Реймеров (Иркутск)

В работе рассматривается задача представления булевых функций полиномиальными формами или просто полиномами, имеющими минимальное число слагаемых. Под сложностью полинома будем понимать число слагаемых в нем, а под сложностью $L(f)$ булевой функции f будем понимать сложность наименьшего из представляющих ее полиномов. В [1] были получены все функции 6 переменных сложности 15. В настоящей работе предлагается алгоритм нахождения

всех функций 6 переменных сложности 14, что позволит понизить верхнюю оценку сложности булевых функций в классе полиномиальных форм для $n \leq 65$.

Разложение Шеннона $f(x_1, \ldots, x_n) = \bar{x}_1 f^0_{x_1} \oplus x_1 f^1_{x_1}$ дает следующую оценку сложности $L(f) \leq L(f^0_{x_1}) + L(f^1_{x_1})$.

Из разложения Шеннона следует, что для получения всех функций 6 переменных сложности 14 достаточно перебрать все возможные комбинации пар функций 5 переменных f_1 и f_2 таких, что $L(f_1) + L(f_2) \geq 14$.

Однако полный перебор потребует порядка 2^{60} операций. Для сокращения перебора можно использовать отношение эквивалентности, сохраняющее сложность полиномов. Наиболее общей из таких эквивалентностей является SP-эквивалентность [2]. Если в качестве f_1 брать представителя класса SP-эквивалентности, а в качестве f_2 — любую булеву функцию, дающую суммарную сложность $L(f_1) + L(f_2) \geq 14$, то общий перебор сокращается до 2^{41} вариантов. Также применение SP-эквивалентности дает следующее свойство: сложность f не превышает суммы сложностей производной $(f^0_{x_1} \oplus f^1_{x_1})$ со сложностями каждой из остаточных.

В качестве исходных данных алгоритма используются предварительно полученные классы SP-эквивалентности для функций 5 переменных (класс определяется представителем и его сложностью). Алгоритм нахождения всех функций от 6 переменых заключается в нахождении кандидатов сложности 14 и дальнейшем исследовании каждого кандидата.

Для поиска функций 6 переменных со сложностью 14 достаточно в качестве остаточных функций в разложении $f(x_1, \ldots, x_n) = \bar{x}_1 f^0_{x_1} \oplus x_1 f^1_{x_1}$ брать пары функций со сложностями (9,9), (9,8), (9,7), (9,6), (9,5), (8,8), (8,7), (8,6), (7,7).

В таблице приведено число SP-классов функций 5 переменных с различной сложностью.

Сложность	Число классов	Число функций
0	1	1
1	1	243
2	4	24 948
3	19	1 351 836
4	137	39 365 190
5	971	545 193 342
6	3572	2 398 267 764
7	2143	1 299 295 404
8	86	11 460 744
9	2	7 824
Всего	6936	4 294 967 296

Как видно из таблицы, пар функций, для которых надо посчитать сложность, достаточно большое число (2^{41}), и вычисление сложности каждой из них алгоритмом точной минимизации займет очень много времени. Однако нет необходимости получать точный минимум для всех кандидатов. Процесс минимизации можно останавливать при получении терма сложности меньше 14. Также в результате экспериментов получено, что подавляющее большинство функций имеют представление термами небольшой сложности. Термы построены по одной из остаточных и производной ($f'_{x_i} = f^0_{x_i} \oplus f^1_{x_i}$).

Алгоритм работает следующим образом: перебираются все функции 5 переменных с заданной сложностью, и для каждой переберираются все представители классов SP-эквивалентности. Для каждой такой пары (представитель класса — функция) по разложению Шеннона и производной вычисляется верхняя оценка сложности для функции, составленной из этих двух. Если верхняя оценка больше либо равна 14, то эта пара заносится в список кандидатов. Полученные кандидаты минимизируются алгоритмом точной минимизации функций 6 переменных.

Результаты отбора представлены следующей таблицей:

Группа	Количество функций
(8,8)	1586
(8,9)	332
(9,9)	992
Всего	2414

Найденные функции образуют 62 SP-класса, которые в сумме содержат 65 393 568 функций.

В [3] показано, что сложность функций от 7 переменных не превосходит 28. Функции 7 переменных сложности 28 можно получить

только из функций 6 переменных сложности 14 и 15. Все функции-кандидаты на сложность 28 получены за 24 часа работы 15 узлов вузовского кластера.

В дальнейшем предполагается исследование на сложность полученных функций.

Работа выполнена при финансовой поддержке РФФИ (проект 09-01-00476-а).

Список литературы

1. Gaidukov A. Algorithm to derive minimum ESOPs for 6-vatiable function // Proceedings of the 5th International Workshop on Boolean Problems. — Freiberg, Germany, 2002. — P. 141–148.

2. Казимиров А. С. Группы операторных преобразований булевых функций // Международная конференция "Алгебра и ее приложения": Тезисы докладов. — Красноярск, 2007. — С. 64–65.

3. Винокуров С. Ф., Казимиров А. С. Верхняя оценка сложности булевых функций в классе ПНФ // Algebra and Model Theory, 4. — Novosibirsk: Novosibirsk State Technical University, 2003. — P. 160–165.

КРИТЕРИЙ КОНЕЧНОСТИ НАДСТРУКТУРЫ НЕКОТОРЫХ КЛАССОВ МОНОТОННЫХ k-ЗНАЧНЫХ ФУНКЦИЙ, СОХРАНЯЮЩИХ ЧАСТИЧНЫЙ ПОРЯДОК С ЕДИНСТВЕННЫМ МИНИМАЛЬНЫМ ЭЛЕМЕНТОМ

В. Б. Ларионов (Москва)

В работе изучается решетка замкнутых относительно суперпозиции классов функций k-значной логики (P_k).

Пусть на $E_k = \{0, 1, \ldots, k-1\}$ задано некоторое отношение частичного порядка r.

Определение 1. Функция $f(x_1, \ldots, x_n)$ называется монотонной относительно частичного порядка r, если для любых двух наборов $\tilde{a}, \tilde{b} \in E_k^n$ таких, что $\tilde{a} \leqslant_r \tilde{b}$, выполнено $f(\tilde{a}) \leqslant_r f(\tilde{b})$. Множество всех функций из P_k, монотонных относительно r, называется монотонным классом M_r.

Для краткости мы будем задавать частичный порядок r частично упорядоченным множеством (ЧУМ) H из элементов E_k, а соответствующий монотонный класс обозначать M_H.

Одним из семейств предполных классов в P_k при $k \geqslant 3$ является семейство $\mathbf{M}$ [3] — подмножество множества всех классов монотонных функций [3]. Известно [4], что монотонный класс является предполным (принадлежит множеству $\mathbf{M}$) тогда и только тогда, когда

частичный порядок, сохраняемый им, обладает в точности одним минимальным и одним максимальным элементом.

Ранее автором изучался вопрос о строении надструктуры монотонных классов, не входящих в семейство **M** [1, 2]. Было показано, что существуют монотонные классы с бесконечной надструктурой, минимальной логикой с подобным классом является P_4, также получены некоторые достаточные для наличия бесконечной надструктуры условия [1].

В данной работе доказывается, что условия из [1] являются также и необходимыми для замкнутых классов монотонных функций, сохраняющих частичный порядок с не более, чем двумя максимальными и двумя минимальными элементами; рассматривается критерий для замкнтутых классов, соответствующих ЧУМ с единственным минимальным и тремя максимальными элементами. Также описываются бесконечные надрешетки замкнутых классов монотонных классов в минимальных логиках.

Введем необходимые понятия.

Определение 2. Пусть a, b, c, d — различные элементы частично упорядоченного множества H. Будем говорить, что указанная четверка удовлетворяет свойству $(*)$, если a, b несравнимы, c, d несравнимы, $c < a$, $d < a$, $c < b$, $d < b$, и не существует последовательности $v_1, \ldots, v_n$ элементов из H, такой что $v_1 = a$, $v_n = b$, для всех $i \in \{1, \ldots, n-1\}$ выполнено $v_i \leqslant v_{i+1}$ или $v_i \geqslant v_{i+1}$, все $v_j > c, d$.

Теорема 1. *Пусть в ЧУМ H есть не более, чем два минимальных и два максимальных элемента. Число различных замкнутых классов k-значной логики, содержащих класс монотонных функций M_H, бесконечно тогда и только тогда, когда в ЧУМ H или его инвертировании найдется четверка элементов, удовлетворяющая свойству $(*)$.*

Рассмотрим ЧУМ $L = \{v_1, v_2, v_3, v_{12}, v_{23}, v_{13}, u_1, u_2\}$, состоящее из восьми элементов, и имеющеет три максимальных (v_1,v_2,v_3). Каждый элемент v_{ij} меньше двух максимумов v_i, v_j (три таких элемента несравнимы между собой). Два минимальных элемента u_1, u_2 меньше всех остальных элементов множества L (и несравнимы между собой).

Теорема 2. *Пусть в ЧУМ H есть единственный минимальный элемент и не более, чем три максимальных. Число различных замкнутых классов k-значной логики, содержащих класс монотонных функций M_H, бесконечно тогда и только тогда, когда в ЧУМ H найдется четверка элементов, удовлетворяющая свойству $(*)$, или подмножество L, причем элементы v_1, v_2, v_3 являются максимумами H, и не существует элемента w такого, что $w \leqslant v_1, v_2, v_3$*

$u\ w \geqslant u_1, u_2$.

Случай, когда ЧУМ H имеет единственный максимальный элемент и не более трех минимальных, аналогичен, и получается инвертированием H.

Минимальной логикой, в которой присутствует класс монотонных функций, сохраняющих ЧУМ H с единственным минимальным элементом, обладающий бесконечной надструктурой, является P_5 [1]. H состоит из трех слоев, состоящих из (сверху вниз) двух, двух и одного элемента, все элементы одного слоя несравнимы, разных слоев — сравнимы. В рассматриваемом случае полностью описана надрешетка класса M_H. Отметим наиболее интересные ее особенности: указанная надрешетка содержится в единственном предполном классе из семейства центральных; M_H предполон в единственном классе, являющимся пересечением всех предикатно-описуемых классов, содержащих M_H; число классов, не являющихся предикатно-описуемыми, бесконечно.

Минимальной логикой, в которой присутствует класс монотонных функций с бесконечной надструктурой, является P_4 [2]. ЧУМ H получается из предыдущего случая выбрасыванием минимального элемента. В данном случае также описана надрешетка замкнутого класса M_H. Рассмотрим некоторые ее особенности: M_H содержится в четырех предполных классах; в надрешетке есть два подмножества, изоморфные рассмотренной бесконечной решетке в P_5; M_H предполнон в единственном предикатно-описуемом классе, являющимся пересечением двух центральных.

Теорема 3. *Пусть в ЧУМ H есть единственный минимальный или максимальный элемент, T — произвольный предикатно-описуемый класс, содержащий M_H и отличный от него. Тогда число различных замкнутых классов, содержащих T, конечно.*

Работа выполнена при поддержке РФФИ, грант 09-01-00701.

Список литературы

1. Ларионов В. Б. О положении некоторых классов монотонных k-значных функций в решетке замкнутых классов // Дискретная математика. —2009. — Т. 21, вып. 5. — С. 111–116.

2. Ларионов В. Б. О монотонных замкнутых классах функций многозначной логики с бесконечной надструктурой // Материалы VII молодежной научной школы по дискретной математике и ее приложениям (18–23 мая 2009 г.). — М.: ИПМ им. М. В. Келдыша РАН, 2009. — С. 7–12.

3. Rosenberg I. La structure des fonctions de plusieur variables sur un ensemble fini // Comptes Rendus, de l'Academ. — Paris, 1965. — 260. — 3817–3819.

4. Мартынюк В. В. Исследование некоторых классов функций в многозначных логиках // Проблемы кибернетики. — 1960. — Вып. 3. — С. 49–61.

О ПОДБИПОЛИГОНАХ БИПОЛИГОНОВ

М. Ю. Максимовский (Москва)

Правым полигоном над полугруппой S (или правым S-полигоном) называется множество X, на котором действует полугруппа S, причем $(xs_1)s_2 = x(s_1s_2)$ при $x \in X$, $s_1, s_2 \in S$ [1]. Аналогичным образом определяется левый полигон. Нетрудно проверить, что переход от полугруппы S к дуальной полугруппе S^{op} (умножение $\circ$ в S^{op} определяется соотношением $s \circ t = ts$) позволяет превратить любой левый S-полигон $(X, \cdot\,)$ в правый S^{op}-полигон $(X, \circ)$, полагая $s \circ x = x \cdot s$. Если на множестве X действует две или более полугрупп, то можно ввести понятие биполигона [1] и мультиполигона. Биполигон ${}_SX_T$ (или (S,T)-биполигон) — это множество, на котором действуют полугруппа S слева и полугруппа T справа, причем действие этих полугрупп перестановочно (т. е. $(sx)t = s(xt)$ при $x \in X$, $s \in S$, $t \in T$). Понятие полигона является алгебраическим выражением автомата Мура [2] $V = (A, Q, \delta)$, где A — входной алфавит; Q — множество состояний; $\delta : Q \times A \to Q$ — функция переходов. Тогда Q можно рассматривать как полигон над полугруппой A_* — полугруппой всех слов в алфавите A, включая пустое слово, если действие A на Q определить по формуле $q \cdot a = \delta(q, a)$, а затем продолжить это действие на элементы из A_* следующим образом: $q \cdot a_{i_1}a_{i_2}...a_{i_m} = (...((qa_{i_1})a_{i_2})...)$. Биполигон можно интерпретировать как автомат с двумя входными алфавитами.

Правый S-полигон называется унитарным, если в полугруппе S есть единица e и $xe = x$ для любого $x \in X$. Аналогично определяются унитарные левые полигоны. (S_1, S_2)-биполигон называется унитарным, если он является унитарным левым S_1-полигоном и одновременно унитарным правым S_2-полигоном.

Подполигоном S-полигона X называется такое подмножество $Y \subseteq X$, что $YS \subseteq Y$. Подбиполигоном (S_1, S_2)-биполигона X называется подмножество $Y \subseteq X$, что $S_1Y \subseteq Y$ и $YS_2 \subseteq Y$. Целью данной работы является описание подбиполигонов биполигонов над некоторыми полугруппами. В работе [4] было получено полное описание строения биполигонов над двумя моноидами. Приведем его.

Теорема 1. *Пусть выполнены условия:* (*a*) ${}_{M_1}Y$, Z_{M_2} — *унитарные полигоны над моноидами* M_1, M_2;

(*b*) $C = Y \cap Z$ — *биполигон, являющийся подполигоном полигонов* Y *и* Z;

(*c*) A — *множество такое, что:* $A \cap (Y \cup Z) = \emptyset$;

(*d*) $X = A \cup Y \cup Z$;

(*e*) $\varphi : X \to Z$ *и* $\psi : X \to Y$ — *такие отображения, что* $\varphi|_Z$ *и* $\psi|_Y$ – *тождественные отображения множеств* Z *и* Y;

(*f*) $\varphi(m_1\psi(x)) = m_1\psi(\varphi(x))$ *и* $\psi(\varphi(x)m_2) = \varphi(\psi(x))m_2$ *при* $x \in X$, $m_1 \in M_1$, $m_2 \in M_2$.

Доопределим действия $M_1 \times Y \to Y$ *и* $Z \times M_2 \to Z$ *до умножения других элементов из* X *на элементы моноидов* M_1 *слева и элементы из* M_2 *справа, полагая*

$$m_1 x = m_1\psi(x)$$

при $m_1 \in M_1$, $x \in X \backslash Y$ *и*

$$xm_2 = \varphi(x)m_2$$

при $m_2 \in M_2$, $x \in X \backslash Z$. *Тогда* X *станет* (M_1, M_2)-*биполигоном. Наоборот, каждый биполигон над моноидами* M_1, M_2 *изоморфен биполигону, полученному таким образом.*

На основе этой теоремы мы получаем теорему, сводящую описание подбиполигонов биполигона над двумя моноидами к описанию подбиполигонов унитарных биполигонов.

Теорема 2. *Пусть* X — (M_1, M_2) *биполигон, где* M_1, M_2 — *моноиды. Подмножество* $Y \subseteq X$ *будет подбиполигоном в том и только том случае, если* Y *можно представить в виде* $Y = E \cup F$, *где* E — *подпиполигон унитарного биполигона* C, $\varphi(F) \subseteq E$ *и* $\psi(F) \subseteq E$.

Список литературы

1. Kilp M., Knauer U., Mikhalev A.V. Monoids, acts and categories. — Berlin — New York: W. de Gruyter, 2000.

2. Кудрявцев В. Б, Подколзин А. С. Введение в теорию абстрактных автоматов. — М.: Изд-во МГУ, 1985.

3. Avdeyev A. Yu., Kozhukhov I. B. Acts over completely 0-simple semigroups // Acta Cybernetica. — 2000. — V. 14, № 4. — P. 523–531.

4. Максимовский М. Ю. О биполигонах и мультиполигонах над полугруппами // Матем. заметки. — В печати.

О СЛОЖНОСТИ НЕКОТОРЫХ k-ЗНАЧНЫХ ФУНКЦИЙ В КЛАССЕ ПОЛЯРИЗОВАННЫХ ПОЛИНОМОВ

Н. К. Маркелов (Москва)

Одним из стандартных способов задания функций k-значной логики являются полиномы. В зависимости от вида слагаемых можно рассматривать обычные, поляризованные и обобщенные полиномы. В настоящей работе рассматриваются поляризованные полиномы для функций 5-значной логики и доказывается несколько утверждений, связанных со сложностью последовательностей периодических функций в указанном классе.

Пусть $E_k = \{0, 1, \ldots, k-1\}$. Функция $f(\tilde{x}^n)$ называется *функцией k-значной логики*, если на всяком наборе $\tilde{\alpha} \in E_k^n$ ее значение содержится в E_k. Совокупность всех функций k-значной логики обозначается P_k.

Поляризованным по вектору поляризации $\sigma = (\sigma_1, \ldots, \sigma_n) \in E_k^n$ *полиномом* P^σ назовем сумму

$$\sum_{\alpha=(a_1,\ldots,a_n)\in E_k^n} c_f^\sigma(\tilde{\alpha}) \cdot (x_1+\sigma_1)^{a_1} \cdot \cdots \cdot (x_n+\sigma_n)^{a_n},$$

где все суммы и произведения берутся по mod k, $c_f^\sigma(\alpha) \in E_k$ — некоторые коэффициенты, и $(x_i+\sigma_i)^{a_i}$ — степени, то есть

$$(x_i+\sigma_i)^{a_i} = 1 \cdot \underbrace{(x_i+\sigma_i) \cdot (x_i+\sigma_i) \cdot \cdots \cdot (x_i+\sigma_i)}_{a_i \text{ раз}}.$$

Каждая функция $f(\tilde{x}^n) \in P_k^n$ представима поляризованным по вектору $\sigma \in E_k^n$ полиномом и единственным образом тогда и только тогда, когда k — простое [1]. Пусть далее k — простое число.

Сложностью $l(P^\sigma)$ полинома, поляризованного по вектору σ, назовем число слагаемых с ненулевыми коэффициентами. Сложность функции k-значной логики в классе поляризованных полиномов определяется как

$$L_k(f) = \min_{\sigma\in E_k^n, P^\sigma = f} l(P^\sigma).$$

Функция Шеннона $L_k(n)$ определяется как сложность самой сложной функции k-значной логики от n переменных в классе поляризованных полиномов:

$$L_k(n) = \max_{f(x_1,\ldots,x_n)\in P_k} (L_k(f)).$$

Известны следующие оценки функций Шеннона:

$$L_2(n) = \left[\frac{2^{n+1}}{3}\right] \text{ [2]}; \quad L_k(1) = k-1 \text{ [3]}; \quad L_k(n) \leqslant \frac{k(k-1)}{k(k-1)+1}k^n \text{ [1]};$$

$$L_k(n) \geqslant (k-1)^n \text{ [3]}; \quad L_3(n) \geqslant \frac{3}{4}3^n \text{ [4]}; \quad L_k(n) \gtrsim \frac{k-1}{k}k^n \text{ [5]}.$$

Последовательность функций

$$\{f_n\} = f_1(x_1), f_2(x_1, x_2), \ldots, f_n(x_1, x_2, \ldots, x_n), \ldots$$

назовем *вырожденной*, если $L_k(f_n) = o(k^n)$ при $n \to \infty$. Последовательности функций, не являющиеся вырожденными, назовем *сложными*.

Будем называть последовательность функций *периодической периода* T если $\exists \tilde{p} \in E_k^T$ такой, что вектор значений каждой из функций имеет вид $\tilde{f}_i = \tilde{p}_{i \,(\mathrm{mod}\, T)}$ для всех i, $i = 0, \ldots, k^n - 1$.

Автором доказаны следующие утверждения:

Теорема 1. *Пусть* $\{f_n\}$, $f_n \in P_5^n$ — *периодическая последовательность периода* 6. *Тогда* $\{f_n\}$ — *вырожденная последовательность.*

Теорема 2. *Пусть* $\{f_n\}$, $f_n \in P_5^n$ — *периодическая последовательность периода* 7 *с периодом* $\tilde{p} = (p_0, \ldots, p_6) : \sum\limits_{i=0}^{6} p_i = 0, \tilde{p} \neq 0$. *Тогда* $L_5(f_n) \geqslant \frac{4}{25}5^n$, *то есть* $\{f_n\}$ — *сложная последовательность.*

Автор благодарит научного руководителя доц. Селезневу С. Н. за постановку задачи и внимание к работе.

Работа выполнена при поддержке РФФИ, грант 09-01-00731.

Список литературы

1. Селезнева С. Н. О сложности представления функций многозначных логик поляризованными полиномами // Дискретная математика. — 2002. — Т. 14, вып. 2. — С. 48–53.

2. Перязев Н. А. Сложность булевых функций в классе полиномиальных поляризованных форм // Алгебра и логика. — 1995. — Т. 34, вып. 3. — С. 323–326.

3. Селезнева С. Н. О сложности поляризованных полиномов функций многозначных логик, зависящих от одной переменной // Дискретная математика. — 2004. — С. 117–120.

4. Денисов Е. Н. О сложности функций трехзначной логики в классе поляризованных полиномов // Дипломная работа. — Кафедра математической кибернетики ф-та ВМиК, 2006.

5. Алексеев В. Б., Селезнева С. Н., Вороненко А. А. О сложности реализации функций k-значной логики поляризованными полиномами // Труды V Международной конференции "Дискретные модели в теории управляющих систем" (Ратмино, 26–29 мая 2003 г.). — М.: МГУ, 2003. — С. 8–9.

О СВОЙСТВАХ ЗАМКНУТЫХ КЛАССОВ ФУНКЦИЙ ТРЕХЗНАЧНОЙ ЛОГИКИ, ПОРОЖДЕННЫХ СИММЕТРИЧЕСКИМИ ФУНКЦИЯМИ

А. В. Михайлович (Москва)

В работе изучаются свойства замкнутых классов функций трехзначной логики. Рассматривается задача о существовании базисов и конечной порожденности для замкнутых классов, порождающие системы которых содержат симметрические функции.

Известно [1], что все замкнутые классы булевых функций имеют конечный базис. На случай многозначных логик этот результат не распространяется. В [2] показано, что при всех $k \geq 3$ в P_k существуют замкнутые классы как со счетным базисом, так и классы, не имеющие базиса. В [3, 4] рассмотрены некоторые семейства замкнутых классов, порожденных симметрическими функциями, и для них приведены критерии базируемости и конечной порожденности. В данной работе рассматриваются классы, порождающие системы которых состоят из симметрических функций и конечного числа функций специального вида. Для отдельных семейств рассматриваемых классов получен критерий базируемости и конечной порожденности. Показано, что задача базируемости для таких классов сводится к задаче базируемости для классов, порожденных симметрическими функциями. Все недостающие определения можно найти в [3–5].

Обозначим через R множество всех функций трехзначной логики, принимающих значения только из множества $\{0, 1\}$ и равных нулю на единичном наборе и на всех наборах, содержащих хотя бы одну нулевую компоненту. Функции f и g из R называются *конгруэнтными*, если одна из них получается из другой переименованием переменных без отождествления. Пусть $f(x_1, \ldots, x_n) \in R$. Будем обозначать через N_f множество всех наборов из E_3^n, на которых функция f

принимает значение 1. Множество $\mathcal{L}$ всех наборов из E_3^n, которые получаются друг из друга перестановкой компонент, называется *слоем*. Функцию $f(x_1, \ldots, x_n)$ из R будем называть *симметрической*, если для любого слоя $\mathcal{L}$ из E_3^n и любых двух наборов $\widetilde{\alpha}$, $\widetilde{\beta}$ из $\mathcal{L}$ выполняется равенство $f(\widetilde{\alpha}) = f(\widetilde{\beta})$. Функцию $f(x_1, \ldots, x_n)$ из R будем называть *m-слойной симметрической функцией*, если существует m различных слоев $\mathcal{L}_1, \ldots, \mathcal{L}_m$, $m \geq 1$, таких, что $N_f = \mathcal{L}_1 \cup \ldots \cup \mathcal{L}_m$. Функцию из R будем называть *монотонной*, если она монотонна относительно порядка $0 < 1 < 2$ на множестве E_3. Множество всех немонотонных m-слойных симметрических функций обозначим через NS^m. Пусть $\widetilde{\alpha} \in E_3^n$. Число единиц в наборе $\widetilde{\alpha}$ обозначим через $|\widetilde{\alpha}|$.

Пусть $f, g \in \mathrm{NS}^m$, $m \geq 1$. Будем говорить, что функция f *не превосходит* функцию g относительно отношения $\preceq$, если $f \in [\{g\}]$. Множество H, $H \subset \mathrm{NS}^m$, $m \geq 1$ называется *цепью*, если любые два элемента множества H сравнимы относительно $\preceq$. Пусть $G \subseteq \mathrm{NS}^m$. Цепь H, $H \subset \mathrm{NS}^m$, $m \geq 1$ называется *максимальной цепью* множества G, если для любой цепи $H_1 \subset \mathrm{NS}^m$, такой, что $H \subseteq H_1$, $H \neq H_1$, цепь H_1 не является подмножеством множества G. Функция $f \in H$ называется *верхней гранью* цепи H, если для любой функции $g \in H$ выполняется неравенство $g \preceq f$. Цепь называется *ограниченной*, если она имеет верхнюю грань.

Имеют место следующие утверждения.

Утверждение 1. *Если множество F содержит счетное число попарно неконгруэнтных немонотонных симметрических функций и $F \subseteq R$, то класс $G = [F]$ не имеет конечного базиса.*

Утверждение 2. *Пусть F — множество попарно неконгруэнтных симметрических функций из R, $G = [F]$, H — конечное множество функций из R, $G_1 = [H \cup F]$. Тогда G_1 имеет базис в том и только в том случае, когда G имеет базис.*

Из утверждений 1 и 2 получаем следующую теорему.

Теорема 1. *Пусть F — множество попарно неконгруэнтных немонотонных симметрических функций, $H = [F]$, G — конечное множество функций из R, $H_1 = [F \cup G]$. Тогда выполняются следующие утверждения.*

(1) *Класс H_1 имеет конечный базис тогда и только тогда, когда класс H имеет конечный базис.*

(2) *Класс H_1 имеет счетный базис тогда и только тогда, когда класс H имеет счетный базис.*

(3) *Класс H_1 не имеет базиса тогда и только тогда, когда класс H не имеет базиса.*

Теорема 1 показывает, что при добавлении к порождающей системе, состоящей из немонотонных симметрических функций, конечного числа функций из R, свойства базируемости и конечной порожденности сохраняются. Используя критерии базируемости и конечной порожденности для m-слойных симметрических функций из [3], получаем следующую теорему.

Теорема 2. *Пусть $F \subseteq \mathrm{NS}^m$, $m \geq 1$, G — конечное множество функций из R, $H = [F \cup G]$. Тогда выполняются следующие утверждения.*

(1) *Класс H имеет конечный базис тогда и только тогда, когда множество F содержит конечное число функций.*

(2) *Класс H имеет счетный базис тогда и только тогда, когда когда F содержит счетное число функций и каждая функция, принадлежащая F, содержится в некоторой конечной максимальной цепи множества F.*

(3) *Класс H не имеет базиса тогда и только тогда, когда F содержит счетное число функций и найдется функция $h \in F$, такая, что h не принадлежит никакой конечной максимальной цепи множества F.*

Автор выражает благодарность профессору А. Б. Угольникову за постановку задачи и постоянное внимание к работе.

Работа выполнена при финансовой поддержке РФФИ (проект 08–01–00863), программы поддержки ведущих научных школ РФ (проект НШ–4437.2010.1) и программы фундаментальных исследований ОМН РАН «Алгебраические и комбинаторные методы математической кибернетики и информационные системы нового поколения».

Список литературы

1. Post E. L. The two-valued iterative systems of mathematical logic // Annals of Math. Studies. — Princeton Univ. Press, 1941. — 5.
2. Янов Ю. И., Мучник А. А. О существовании k-значных замкнутых классов, не имеющих конечного базиса // ДАН СССР. — 1959. — Т. 127, № 1. — С. 44–46.
3. Михайлович А. В. О замкнутых классах трехзначной логики, порожденных симметрическими функциями // Вестник Моск. ун-та. Сер. 1. Математика. Механика. — 2008. — № 4. — С. 54–57.
4. Михайлович А. В. О классах функций трехзначной логики, порожденных монотонными симметрическими функциями // Вестник Моск. ун-та. Сер. 1. Математика. Механика. — 2009. — № 1. — С. 33–37.

5. Яблонский С. В. Введение в дискретную математику. — М.: Высшая школа, 2001.

ОБ ОБОБЩЕНИЯХ КЛОНОВ С МАЖОРИТАРНОЙ ФУНКЦИЕЙ

Н. Г. Парватов (Томск)

В связи с проблемой конечной порождаемости рассматриваются некоторые обобщения клонов с мажоритарной функцией.

Будем рассматривать функции зависящие от конечного числа переменных и вместе с ними принимающие значения в конечном множестве E. Множество всех таких функций обозначается через P_E. *Клоном* называется всякое множество функций из P_E, содержащее селекторы (функции, совпадающие с некоторым своим аргументом) и замкнутое операциями суперпозиции [1]. Клон называется *конечно-порождаемым*, если все его функции можно получить с использованием операций суперпозиции из некоторого конечного его подмножества. Представляет интерес *проблема конечной порождаемости* клона, состоящая в выявлении условий, при которых он является конечно-порождаемым. Некоторые такие условия будут сформулированы далее. Понадобятся некоторые определения.

Обозначим через Π_E множество предикатов $P : E^n \to \{\text{И, Л}\}$ при всевозможных натуральных n. Напомним, что множество $inv_E(X)$ предикатов из Π_E, сохраняемых всеми функциями множества $X \subseteq P_E$, содержит все диагонали (тождественно истинные или ложные предикаты, а также предикаты $x_i = x_j \wedge \ldots \wedge x_k = x_l$ при $\{i, j, \ldots, k, l\} = \{1, \ldots, n\}$ и натуральных n) и замкнуто операциями проектирования и конъюнкции предикатов, отождествления и перестановки переменных, а также операциями введения и удаления фиктивных переменных [2]. В связи с этим представляют интерес совокупности предикатов, содержащие диагонали и замкнутые операциями конъюнкции, отождествления и перестановки переменных, введения и удаления фиктивных пременных. Такие совокупности станем называть *и-классами*. Для любого множества Y предикатов из Π_E через $[Y]_\wedge$ станем обозначать *и-класс, порождённый множеством* Y, то есть наименьший по включению среди включающих множество Y. Через $Y^{(d)}$ обозначается множество предикатов из Y, зависящих не более, чем от d переменных. Имеет место

Теорема 1. *Пусть задано натуральное* $d \geq 2$. *Для клонов* M_1 *и* M_2 *следующие условия равносильны:*

(1) *имеет место включение* $M_1 \subseteq M_2$ *и для любой функции* $f(x_1, \ldots, x_n)$ *из* M_2 *найдётся функция* $m_f(x_1, \ldots, x_{n+d+1})$ *в* M_1, *удовлетворяющая соотношениям*

$$f(x) = m_f(x, f(x), \ldots, f(x), x_{n+i}, f(x), \ldots, f(x)),$$

где через x *обозначен набор переменных* $x_1, \ldots, x_n$, *переменная* x_{n+i} *находится на* $(n+i)$*-м месте функции* m_f *и* $1 \leq i \leq d+1$;

(2) *имеет место равенство*

$$inv_E(M_1) = [inv_E(M_2) \cup (inv_E(M_1))^{(d)}]_\wedge.$$

Клон M_1 называется d-*подклоном* клона M_2, если выполняются условия (1) и (2) из теоремы 1. Такие клоны представляют интерес в связи с проблемой конечной порождаемости, так как имеет место

Теорема 2. *Клон, содержащий конечно-порождаемый* d*-подклон, сам конечно-порождаемый.*

Если в условии (1) теоремы 1 функцию m_f всегда удаётся выбрать зависящей не более чем от c переменных функции f, то M_1 называется (c,d)-*подклоном* клона M_2 и оба эти клона называются (c,d)-*клонами*. Отметим, что $(0,d)$-клонами являются в точности клоны, содержащие $(d+1)$-местную мажоритарную функцию $m(x_1, \ldots, x_{d+1})$, удовлетворяющую в соответствии с определением соотношениям $x = m(x, \ldots, x, x_i, x, \ldots, x)$, где переменная x_i находится на i-м месте функции m, а переменная x — на остальных местах и $1 \leq i \leq d+1$. Клоны с мажоритарной функцией охарактеризованы теоремой Бейкера и Пиксли в [3], широко известна конечная порождаемость таких клонов, [4]. Обобщает этот факт

Теорема 3. *Всякий* (c,d)*-клон конечно-порождаемый.*

Заметим, что d-подклоны в соответствии с теоремой 1 имеют два определения, а (c,d)-клоны были определены только одним способом. Исправляет ситуацию следующая

Теорема 4. *Для любых натуральных* c *и* d *таких, что* $d \geq 2$, *и любых клонов* M_1 *и* M_2 *равносильны условия:*

(1) *клон* M_1 *является* (c,d)*-подклоном клона* M_2;

(2) *клон* M_1 *является* d*-подклоном клона* M_2 *и всякая функция из* M_2 *по некоторому набору своих переменных, содержащему не более* c *переменных, сохраняет все редуцированные предикаты из* $inv_E(M_2)$, *зависящие более чем от* d *переменных.*

При этом m-местный предикат p из Π_E называется *редуцированным*, если некоторый набор Y из E^m не удовлетворяет этому предикату, но для любого $i, 1 \leq i \leq m$, некоторый набор, отличающийся от

Y только i-й компонентой, удовлетворяет предикату p. Сохранение функций $f(x_1, \ldots, x_n)$ m-местного предиката p по набору переменных $x_{i_1}, \ldots, x_{i_c}$ означает, что для любых наборов $y_i = (y_{i,1}, \ldots, y_{i,m})$ из E^m при $1 \leq i \leq n$ верно следующее: если наборы $y_{i_1}, \ldots, y_{i_c}$ удовлетворяют предикату p, то и набор

$$(f(y_{1,1}, \ldots, y_{n,1}), \ldots, f(y_{1,m}, \ldots, y_{n,m}))$$

удовлетворяет этому предикату.

Работа выполненая в рамках реализации ФЦП "Научные и научно-педагогические кадры инновационной России" на 2009–2013 годы.

Список литературы

1. Мальцев А. И. Итеративные алгебры Поста. — Новосибирск: Изд-во НГУ, 1976.

2. Боднарчук В. Г., Калужнин Л. А., Котов В. Н., Ромов Б. А. Теория Галуа для алгебр Поста // Кибернетика. — 1969. — № 3. — С. 1–10; № 5. — С. 1–9.

3. Baker K. A., Pixly A. F. Polynomial interpolation and Chinese remainder theorem for algebraic systems // Math. Zeiteschr. — 1975. — Bd. 143, № 2. — S. 165–174.

4. Марченков С. С. К существованию конечных базисов в замкнутых классах булевых функций // Алгебра и логика. — 1984. — Т. 23, № 1. — С. 88–99.

КОМПОЗИЦИОННАЯ МОДЕЛЬ ПОСЛЕДОВАТЕЛЬНЫХ СВЯЗЕЙ В ИНФОРМАЦИОННЫХ СИСТЕМАХ

Т. С. Парфирова (Киев)

Создание сложных программных систем включает в себя построение потоков данных между подсистемами. Эта работа посвящена моделированию важного частного случая — последовательных потоков. Такое сужение вполне обусловлено прагматикой: структуры типа цикла и ветвления обычно характеризируют строение программы на микроуровне, они инкапсулированы внутри небольших программных единиц, а поток данных между такими единицами можно считать линейным.

Моделирование последовательных структур программ на основе суперпозиции (умножения) унарных функций не вполне адекватно отражает суть явления, ведь подсистема в последовательной системе может получать на вход не все, а некоторую часть данных от

непосредственно предшествующей подсистемы, т. е. может игнорировать часть поступающего на вход потока данных. Помимо этого, поток данных с выхода некоторой подсистемы может передаваться по частям различным последующим подсистемам, как заданным априори, так и определяемым динамически, что также трудно смоделировать в терминах суперпозиции унарных функций.

В соответствии с композиционным подходом и разработанной на его основе сущностной платформой [1, 2] данные моделируются именными множествами (ИМ), а подсистемы — именными функциями (ИФ), определения которых даны ниже. Обозначим через $\mathbf{D}$ и $\mathbf{V}$ множество всех денотатов и имен соотвественно. V-именным множеством называют отношение $\alpha \in \mathbf{D}^V$, $V \subseteq \mathbf{V}$. Через $\mathcal{N}$ обозначим множество всех ИМ. Так как композиционное програмирование имеет дело с моделированием реальных данных, то всюду далее расматриваемтолько финитные объекты, в частности V-именные множества при конечных V.

Над ИМ определены следующие основные операции:

именование: $v \Leftarrow (d) = \{(v, d)\}$;

разыменование: $v \Rightarrow (\alpha) = \begin{cases} d \text{ при } (v,d) \in \alpha, \\ \text{не определено} \end{cases}$

Пусть α и β — ИМ, тогда *наложение* ИМ определяется так:

$$\alpha \nabla \beta = \beta \cup \{(u, d) \mid (u, d) \in \alpha, u \notin pr_1(\beta)\}.$$

ИФ — унарная функция вида $\mathcal{N} \widetilde{\to} \mathcal{N}$. ИФ f называется V-арной, если $\mathrm{dom}\, f \subseteq \mathbf{D}^V$, и (V, W)-арной, если к тому же $\mathrm{rang} f \subseteq \mathbf{D}^W$. Именная функция, обладающая какой-либо арностью, называется *полиарной*. Всюду далее рассматриваются только полиарные ИФ.

Композиции *умножения* и *наложения* функций определяются следующим образом:

$$(f \circ g)(\alpha) \simeq g(f(\alpha)),$$
$$(f \nabla g)(\alpha) \simeq f(\alpha) \nabla g(\alpha).$$

Ограничением назовем $(V, U \cap V)$-арную ИФ $\uparrow_U^V$ (где V, $U \subseteq \mathbf{V}$), такую, что

$$\uparrow_U^V (\alpha) = \{(u, d) | (u, d) \in \alpha \wedge u \in U\}, \text{ при } \alpha \in \mathbf{D}^V.$$

Переименованием назовем (V, U)-арную ИФ $\updownarrow^\xi$, где $U, V \subseteq \mathbf{V}$; $\xi : U \to V$, такую что $\updownarrow^\xi (\alpha) = \{(u, \xi(u) \Leftarrow (\alpha)) \mid u \in U\}$, при $\alpha \in \mathbf{D}^V$.

Обозначим $\delta_V = \{(v, v) \mid v \in V\}$.

Последовательно-параллельной ИФ в базисе Φ (где Φ – некоторое семейство ИФ) называется такая ИФ f, что

$$f \in [\Phi \cup \{id_{\mathbf{D}^V} | V \subseteq \mathbf{V}\} \cup \{\uparrow_U^V | U, V \subseteq \mathbf{V}\} \cup \{\updownarrow^\xi | \xi \in V^U,\ U, V \subseteq \mathbf{V}\}]_{\{\circ, \nabla\}}$$

Звеном с ядром f назовём ИФ вида

$$h = \updownarrow^\xi \nabla (\uparrow_{pr_2(\zeta)}^{pr_2(\xi)} \circ \updownarrow^\zeta \circ f),$$

где $\xi, \zeta : \mathbf{V} \widetilde{\to} \mathbf{V}$. Звено будем обозначать также через $\mathcal{L}_{\zeta}^{\xi}(f)$.

Цепочной функцией в базисе Φ называется функция вида

$$h = h_1 \circ h_2 \circ \ldots \circ h_n,$$

где h_i — звено в базисе Φ ($i = \overline{1,n}$). Если g и h — цепочные функции, то $g \circ h$ — также цепочная функция.

Пусть дана цепочная функция $h = h_1 \circ h_2 \circ \ldots \circ h_n$, причем звено h_i цепочной функции h имеет арность (U_i, V_i) и вид $\mathcal{L}_{\zeta_i}^{\xi_i}(f_i)$ ($i = \overline{1,n}$), $W \subseteq \mathbf{V}$, $W \cap U_i = \emptyset$ и $W \cap V_i = \emptyset$ для всех $i = \overline{1,n}$ (в этом случае будем говорить, что имена из W не входят в h).

Расширением ИФ h (обозначим $\mathcal{X}^W(h)$) назовём композицию, которая ИФ h ставит в сотвествие новую цепочную функцию h', строящуюся из h слеюующим образом:

$$h' = h'_1 \circ h'_2 \circ \ldots \circ h'_n,$$
$$h'_i = \mathcal{L}_{\zeta_i}^{\xi_i \cup \delta_W}(f_i).$$

Если цепочная функция h является (U,V)-арной, а множество W состоит из имен, не входящих в h, и $h' = \mathcal{X}^W(h)$ то

$$h' = (\uparrow_W^{U \cup W} \circ id_{D^W}) \nabla (\uparrow_U^{U \cup W} \circ h).$$

Имеет место дистрибутивность расширения относительно суперпозиции. Пусть даны цепочные функции g и h и произвольное множество имен W, не входящих ни в g, ни в h. Тогда

$$\mathcal{X}^W(g \circ h) = \mathcal{X}^W(g) \circ \mathcal{X}^W(h).$$

Пусть h – U-арная цепочная функция, $h = h_1 \circ \ldots \circ h_n$, где $h_i = \mathcal{L}_{\zeta_i}^{\xi_i}(f_i)$ для $i = \overline{1,n}$, $\hat{U}$ — некоторое множество имен, не входящих в h, и φ — взаимно однозначное отображение вида $\hat{U} \to U$.

Композицией резервирования назовем такую композицию, которая ставит цепочной функции h в соответствие новую цепочную функцию $h' = \mathcal{C}_h^{\varphi}$, строящуюся следующим образом:

$$h' = \mathcal{L}_{\zeta_1}^{\xi_1 \cup \varphi}(f_1) \circ \ \mathcal{X}^{\hat{U}}(h_2 \ldots \circ h_n).$$

Лемма. *Если h — U-арная цепочная функция, множество $\hat{U}$ и отображение φ удовлетворяют условиям из определения резервирования, то для любого U-именного множества α имеет место*

$$\mathcal{C}_h^{\varphi}(\alpha) = h(\alpha) \cup \{(\varphi^{-1}(u), d) \mid (u,d) \in \alpha\}.$$

Теорема 1. *Пусть g и h — соответственно (U,V')-арная и (U,V'')-арная цепочные функции. Тогда существует $W \subseteq \mathbf{V}$ и цепочная функция f с арностью (U,W), такая, что $f \circ \uparrow_{V' \cup V''}^{W} = g \nabla h$.*

Легко видеть, что этому условию удовлетворяет функция

$$f = \mathcal{C}_g^{\varphi} \circ \mathcal{L}_{\emptyset}^{\varphi^{-1} \cup \psi}(id_{D^{\emptyset}}) \circ \mathcal{X}^{\hat{V'}}(h) \circ \mathcal{L}_{\delta_{V''}}^{\psi^{-1} \cup \delta_{\hat{V'}} \cup V'' \setminus V'}(id_{D^{V''}}),$$

где $\hat{U} \subseteq \mathbf{V}$ (имена из $\hat{U}$ не входят ни в g, ни в h); $\varphi : \hat{U} \to U$ — взаимно однозначное отображение; $\hat{V'} \subseteq \mathbf{V}$ (имена из $\hat{V'}$ не входят в g), $\hat{V'} \cap \hat{U} = \emptyset$; $\psi : \hat{V'} \to V'$ — взаимно однозначное отображение, при $X = V \cup W \cup \hat{V}$.

Из свойства дистрибутивности расширения относительно суперпозиции следует основной результат:

Теорема 2. *Какова бы ни была (U,V)-арная последовательно-параллельная функция f в базисе Φ, существует такая цепочная функция $\hat{f}$ с арностью $(U,\hat{V})$, $V \subseteq \hat{V}$, в том же базисе, что $f = \hat{f} \circ \uparrow_V^{\hat{V}}$.*

Список литературы

1. Никитченко Н. С. Композиционные логики номинативных данных // Проблемы программирования. — 2003. — № 3. — С. 29–40.

2. Редько В. Н. Экзистенциальные основания композиционной парадигмы // Кибернетика и системный анализ. — 2008. — № 2. — С. 3–12.

КЛАССИФИКАЦИЯ УНАРНЫХ КЛОНОВ РАНГА 3

Н. А. Перязев, С. В. Криштофенко (Иркутск)

Напомним, что клоном на множестве A называют множество операций на A замкнутое относительно суперпозиции и содержащее все проекции. Ранг клона определяется как мощность множества A. Изучение решетки замкнутых множеств операций начато в работах Э. Поста. Из его работы [1] следует описание решетки клонов ранга 2, которая оказалась счетной. Решетки клонов ранга больше 2 являются континуальными. Полное описание этих решеток отсутствует даже для ранга 3, хотя в последние время проводятся интенсивные исследования.

Одним из способов изучения решетки клонов является разбиение этой решетки на множество попарно непересекающихся интервалов. После этого каждый интервал можно исследовать отдельно. Известно [2], что решетку клонов ранга k можно разбить на непересекающиеся интервалы, число которых совпадает с числом унарных клонов этого ранга. Интервалы, состоящие из всех клонов, содержащих одно и тоже множество унарных операций называют моноидальными. При этом число требуемых изучения моноидальных интервалов можно уменьшить за счет рассмотрения только попарно

не изоморфных интервалов. Так решетка клонов ранга 2 разбивается на 6 моноидальных интервалов, среди которых 5 попарно не изоморфных. Впрочем, эту решетку можно разбить и на 3 непересекающихся попарно не изоморфных интервала.

Поэтому, вызывает интерес нахождения множества унарных клонов такого, что все остальные унарные клоны определяют моноидальные интервалы изоморфные хоть одному моноидальному интервалу, определяемому унарным клоном из этого множества. Множество этих клонов так же желательно представить в виде объединения попарно непересекающихся интервалов в решетке унарных клонов. Ниже эти задачи решаются для клонов ранга 3.

В книге [3] приведено описание всех 699 унарных клонов ранга 3 (попутно заметим, что в этой книге в таблице унарных клонов допущено 3 опечатки).

Множество всех унарных клонов ранга 3 разбивается на 43 попарно непересекающиеся интервала, 13 из которых имеют по 3 изоморфные копии. В 17 интервалах, в сумме содержится 239 клонов. Получили, что для полного изучения моноидальных интервалов в решетке клонов ранга 3 достаточно исследовать только 239 из них. Ниже приведем эти 17 интервалов.

Следуя [3], введем обозначения для всех унарных операций (определяя их векторным заданием):

$c_0 = (0,0,0)$, $c_1 = (1,1,1)$, $c_2 = (2,2,2)$,
$s_1 = (0,1,2)$, $j_0 = (1,0,0)$, $u_0 = (2,0,0)$, $v_0 = (2,1,1)$,
$s_2 = (0,2,1)$, $j_1 = (0,1,0)$, $u_1 = (0,2,0)$, $v_1 = (1,2,1)$,
$s_3 = (1,0,2)$, $j_2 = (0,0,1)$, $u_2 = (0,0,2)$, $v_2 = (1,1,2)$,
$s_4 = (1,2,0)$, $j_3 = (1,1,0)$, $u_3 = (2,2,0)$, $v_3 = (2,2,1)$,
$s_5 = (2,0,1)$, $j_4 = (1,0,1)$, $u_4 = (2,0,2)$, $v_4 = (2,1,2)$,
$s_6 = (2,1,0)$, $j_5 = (0,1,1)$, $u_5 = (0,2,2)$, $v_5 = (1,2,2)$.

Для определения интервалов необходимы обозначения для 30 унарных клонов:

$U_0 = \{s_1\}$, $U_1 = \{s_1, c_0 - c_2\}$, $U_2 = \{s_1, c_0 - c_2, j_0 - j_5, u_0 - u_5, v_0 - v_5\}$,
$U_3 = \{s_1, s_4, s_5\}$, $U_4 = \{s_1 - s_6, c_0 - c_2, j_0 - j_5, u_0 - u_5, v_0 - v_5\}$,
$U_5 = \{s_1, j_5\}$, $U_6 = \{s_1, s_2, j_0, j_5, u_0, u_5\}$, $U_7 = \{s_1, v_2\}$,
$U_8 = \{s_1, s_2, v_1 - v_4\}$, $U_9 = \{s_1, s_2\}$, $U_{10} = \{s_1, c_0\}$,
$U_{11} = \{s_1, s_2, c_0, j_1, j_2, j_5, u_1, u_2, u_5\}$, $U_{12} = \{s_1, c_1, c_2\}$,
$U_{13} = \{s_1, s_2, c_1, c_2, j_5, v_0 - v_5\}$, $U_{14} = \{s_1, s_2, c_0 - c_2\}$,
$U_{15} = \{s_1, s_2, c_0 - c_2, j_0 - j_5, u_0 - u_5, v_0 - v_5\}$, $U_{16} = \{s_1, c_0 - c_2, v_2\}$,
$U_{17} = \{s_1, j_0, j_5, c_0 - c_2, v_0 - v_5\}$, $U_{18} = \{s_1, c_0 - c_2, j_5, b_5, v_2\}$,
$U_{19} = \{s_1, c_0 - c_2, j_0, j_5, u_0, u_5, v_0 - v_5\}$, $U_{20} = \{s_1, c_0 - c_2, v_4\}$,
$U_{21} = \{s_1, c_0 - c_2, j_1, j_4, v_1, v_4\}$, $U_{22} = \{s_1, c_0 - c_2, u_1, v_4\}$,

$U_{23} = \{s_1, c_0 - c_2, j_1 - j_4, u_1 - u_4, v_1 - v_4\}$, $U_{24} = \{s_1, c_0 - c_2, u_4\}$,
$U_{25} = \{s_1, c_0 - c_2, j_1, j_3, u_2, u_4, v_2, v_4\}$, $U_{26} = \{s_1, c_0 - c_2, j_1, u_1\}$,
$U_{27} = \{s_1, c_0 - c_2, j_0 - j_5, u_0 - u_5\}$, $U_{28} = \{s_1, c_0 - c_2, u_1\}$,
$U_{29} = \{s_1, c_0 - c_2, u_0, u_1, u_4, u_5\}$.

Ниже перечисляются 17 попарно непересекающихся искомых интервала решетки унарных клонов ранга 3:
$I_1 = [U_0, U_0]$, $I_2 = [U_1, U_1]$, $I_3 = [U_2, U_2]$, $I_4 = [U_3, U_4]$, $I_5 = [U_9, U_9]$,
$I_6 = [U_5, U_6 1]$, $I_7 = [U_7, U_8]$, $I_8 = [U_{10}, U_{11}]$, $I_9 = [U_{12}, U_{13}]$,
$I_{10} = [U_{14}, U_{15}]$, $I_{11} = [U_{16}, U_{17}]$, $I_{12} = [U_{18}, U_{19}]$, $I_{13} = [U_{20}, U_{21}]$,
$I_{14} = [U_{22}, U_{23}]$, $I_{15} = [U_{24}, U_{25}]$, $I_{16} = [U_{26}, U_{27}]$, $I_{17} = [U_{28}, U_{29}]$.

При этом интервалам $I_5 - I_{17}$ соответствуют еще по две изоморфные копии, клоны которых определяют изоморфные моноидальные интервалы. Отметим, что интервалы I_1, I_2, I_3, I_5 состоят из 1 клона, интервал I_{13} из 4 клонов, интервалы I_7, I_{17} из 5 клонов, интервалы I_4, I_6 из 6 клонов, интервал I_{12} из 9 клонов, интервал I_{15} из 11 клонов, интервалы I_{10}, I_{14} из 16 клонов, интервал I_{16} из 24 клонов, интервал I_{11} из 27 клонов, интервал I_8 из 33 клонов, интервал I_9 из 73 клонов.

Работа выполнена при финансовой поддержке РФФИ (проекты 07-01-00240 и 09-01-00476).

Список литературы

1. Post E. Two-valued iterative systems of mathematical logic // Annals of Math. Studies. — Princeton: Univ. Press, 1941. — V. 5.

2. Szendrei A. Clones in universal algebra // Seminare de Mathematique Superieures. — Montreal: Let Presses de Universite de Montreal, 1986.

3. Lau D. Function Algebras on Finite Sets. — Springer-Verlag Berlin YeideWater Resourses Research, 2006.

АЛГОРИТМ НАХОЖДЕНИЯ ПРЕДСТАВЛЕНИЯ МУЛЬТИОПЕРАЦИЙ МИНИМАЛЬНОЙ СТАНДАРТНОЙ ФОРМОЙ

Н. А. Перязев, И. А. Яковчук (Иркутск)

Пусть $B(A)$ — множество всех подмножеств A, в том числе $\emptyset$. Отображение из A^n в $B(A)$ называется n-местной мультиоперацией на A. Для множества всех n-местных мультиопераций на A используем обозначение H_A^n, при $|A| = k$, соответственно, H_k^n.

Суперпозиция мультиопераций определяется следующим образом

$$(f * (f_1, ..., f_n))(a_1, ..., a_m) = \bigcup_{b_i \in f_i(a_1,...,a_m)} f(b_1, ..., b_n).$$

Мультиоперации f на $A = \{a_0, ..., a_{k-1}\}$ можно представлять как отображения

$$f : \{2^0, 2^1, ..., 2^{k-1}\}^n \to \{0, 1, ..., 2^k - 1\},$$

получаемых из f при кодировке

$$a_i \to 2^i; \quad \emptyset \to 0; \quad \{a_{i_1}, ..., a_{i_s}\} \to 2^{i_1} + ... + 2^{i_s}.$$

При этом n-местную мультиоперацию f задаем векторной формой $(\alpha_1, ..., \alpha_{k^n})$, где $f(a_1, ..., a_n) = \alpha_i$ и $(a_1 - 1, ..., a_n - 1)$ есть представление i в системе исчисления по основанию k.

Мультиоперация $\cap$, называемая пересечением, определяется так $\cap(a, b) = \{a\} \cap \{b\}$. Как принято для бинарных операций используем суфиксную форму записи $\cap(a, b) = (a \cap b)$. Очевидно, что эта операция коммутативна и ассоциативна. Поэтому, как обычно, несущественные скобки будем опускать.

Следующие мультиоперации $p \in H_k^1$ и $d_{i,\alpha}^n \in H_k^n$ определим через их векторное задание

$$p = (2, 4, ..., 2^k - 1, 1);$$

$$d_{i,\alpha}^n = (2^k - 1, ..., 2^k - 1, \overset{i}{\alpha}, 2^k - 1, ..., 2^k - 1), \quad (1 \le i \le k^n),$$

где $\alpha \in \{0, ..., 2^k - 2\}$. В частности $d_{1,\alpha}^0 = (\alpha)$.

Пусть $f \in H_k^n$. Тогда следуя [1] следующее представление назовем *стандартной формой* мультиоперации

$$f(x_1, ..., x_n) = \bigcap_j d_j(x_{i_1}, ..., x_{i_m}),$$

где $d_j \in \{d_{i,\alpha}^m \mid 0 \le m \le n, \alpha \in \{0, ..., 2^k - 2\}\}$.

Представим мультиоперацию $f \in H_2^n$, заданной векторно $f(x_1, x_2, x_3) = (32323030)$, стандартной формой.

$$f = d_{2,2}^3(x_1, x_2, x_3) \cap d_{4,2}^3(x_1, x_2, x_3) \cap d_{6,0}^3(x_1, x_2, x_3) \cap d_{8,0}^3(x_1, x_2, x_3).$$

В то же время

$$f = d^1_{2,2}\ (x_3) \cap d^2_{4,1}\ (x_1, x_3).$$

Как видим, представление мультиопераций стандартной формой не единственно.

Представление мультиопераций специальными стандартными формами изучались в [1]. В данном сообщении рассмотрим минимизацию мультиопераций в классе стандартных форм.

Количество компонент пересечения в представлении назовем его сложностью. Под минимальной стандартной формой будем понимать представление мультиоперации в виде стандартной формы с наименьшей сложностью.

Ниже приводится алгоритм, позволяющий найти минимальное представление мультиопераций в классе стандартных форм, основанный на минимизации булевых функций в классе ДНФ.

На вход алгоритма подается вектор $\widetilde{\alpha}$, представляющий мультиоперацию f.

На выходе алгоритма получим минимальную стандартную форму, представляющую мультиоперацию f.

Перейдем к описанию алгоритма.

Шаг 1. Рассмотрим все представления $f \in H^n_k$ вида:

$$f = h^0_{i_0} \cap h^1_{i_1} \cap h^2_{i_2} \cap ... \cap h^{2^k-2}_{i_{2^k-2}},$$

где $h^s_{i_s} = (\alpha_1, ..., \alpha_{k^n}), \alpha_i \in \{s, 2^k - 1\}, s \in \{0, ..., 2^k - 2\}$.

Шаг 2. По каждой $h^s_{i_s} = (\alpha_1, ..., \alpha_{k^n})$ определим булеву функцию $f^s_{i_s} = (\beta_1, ..., \beta_{k^n})$, где $\beta_i = \begin{cases} 1, & \text{если } \alpha_i \neq 2^k - 1; \\ 0, & \text{если } \alpha_i = 2^k - 1. \end{cases}$

Шаг 3. Для каждой $f^s_{i_s}$ вычислим сложность кратчайшей ДНФ.

Шаг 4. Выберем представление, которому будет соответствовать минимальная суммарная сложность. Представления мультиоперации с наименьшей сложностью, записанное в стандартной форме и будет выходом алгоритма.

Для того, чтобы перейти от булевых функций к записи представления мультиоперации в стандартной форме необходимо каждой элементарной конъюнкции, входящей в кратчайшие ДНФ булевых функций f_s, где $s \in \{0, 1, ..., 2^k - 2\}$ поставить в соответствие функцию $d_j(x_{i_1}, ..., x_{i_m})$, такую что $d_j \in \{d^m_{i,s} \mid 0 \leq m \leq n, \}$.

Тогда представление вида

$$f(x_1, ..., x_n) = \bigcap_j d_j(x_{i_1}, ..., x_{i_m}),$$

является минимальной стандартной формой мультиоперации f.

На основе описанного алгоритма создана программная реализация минимизации мультиопераций на 2-х элементном множестве в классе стандартных форм и проведены компьютерные эксперименты.

Работа выполнена при финансовой поддержке РФФИ (проекты 07-01-00240 и 09-01-00476).

Список литературы

1. Перязев Н. А. Суперклоны мультиопераций // Труды VIII Международной конференции "Дискретные системы в теории управляющих систем". — М.: МАКС Пресс, 2009. — С. 233–238.

О НАХОЖДЕНИИ КОЭФФИЦИЕНТОВ ОБОБЩЕННО-ПОЛЯРИЗОВАННЫХ ПОЛИНОМОВ k-ЗНАЧНЫХ ФУНКЦИЙ

С. Н. Селезнева (Москва)

В настоящей заметке предлагаются формулы для подсчета коэффициентов обобщенно-поляризованных полиномов k-значных функций.

Пусть $k \geq 2$, $E_k = \{0, 1, \ldots, k-1\}$. Под k-значной функцией будем понимать отображение $f^n : E_k^n \to E_k$, $n = 0, 1, \ldots$. Множество всех k-значных функций обозначим как P_k.

Будем рассматривать сложение и умножение по mod k при простых k.

Каждая k-значная функция $f(x_1, \ldots, x_n)$ может быть однозначно задана *полиномом* по mod k (при простых k) [1], то есть в виде

$$f(x_1, \ldots, x_n) = \sum_{\alpha=(a_1,\ldots,a_n)\in E_k^n} c_f(\alpha) x_1^{a_1} \cdot \cdots \cdot x_n^{a_n},$$

где $x_i^{a_i} = \prod_{j=1}^{a_i} x_i$, $x_i^0 = 1$ – степени, а $c_f(\alpha) \in E_k$ – коэффициенты.

Степенью функции $f(x_1, \ldots, x_n)$ назовем степень задающего ее полинома по mod k, то есть число $d(f) = \max\limits_{c_f(\alpha)\neq 0} \sum\limits_{i=1}^{n} a_i$.

Введем понятие обобщенно-поляризованного полинома.

Пусть $D_m = \{f(x) \in P_k | d(f) = m\}$, $m = 0, 1, \ldots, k-1$ и $\tilde{D}_k = D_{k-1} \times \cdots \times D_1 \times D_0$.

Обобщенным вектором поляризации назовем вектор

$$\delta = (\delta_1, \ldots, \delta_n) \in \tilde{D}_k^n,$$

в котором

$$\delta_i = (s_{i,k-1}(x_i), \ldots, s_{i,1}(x_i), s_{i,0}(x_i)) \in \tilde{D}_k,$$

то есть степень полинома $s_{i,m}(x_i)$ равна m.

Каждая k-значная функция $f(x_1, \ldots, x_n)$ может быть однозначно задана *обобщенно-поляризованным полиномом* по вектору δ (при простых k) [2], то есть в виде

$$f(x_1, \ldots, x_n) = \sum_{\alpha=(a_1,\ldots,a_n)\in E_k^n} c_f^\delta(\alpha) s_{1,a_1}(x_1) \cdot \cdots \cdot s_{n,a_n}(x_n),$$

где $c_f^\delta(\alpha) \in E_k$ — коэффициенты.

Отметим некоторые особенности обобщенно-поляризованных полиномов.

Обобщенно-поляризованный полином для функции $f(x_1, \ldots, x_n) \in P_k$ по обобщенному вектору поляризации

$$\delta = ((x_1^{k-1}, \ldots, x_1, 1), \ldots, (x_n^{k-1}, \ldots, x_n, 1)) \in \tilde{D}_k^n$$

является обычным полиномом $\bmod k$.

Поляризованный полином для функции $f(x_1, \ldots, x_n) \in P_k$ по вектору поляризации $(d_1, \ldots, d_n) \in E_k^n$ является частным случаем обобщенно-поляризованного полинома по обобщенному вектору поляризации

$$\delta = (((x_1+d_1)^{k-1}, \ldots, x_1+d_1, 1), \ldots, ((x_n+d_n)^{k-1}, \ldots, x_n+d_n, 1)) \in \tilde{D}_k^n.$$

Для булевых функций обобщенно-поляризованные полиномы совпадают с поляризованными полиномами.

Известны быстрые алгоритмы нахождения коэффициентов различных полиномов по значениям функции. Для булевых функций быстрый алгоритм нахождения коэффициентов полинома по $\bmod 2$ описан в [3]. Алгоритм построения поляризованных полиномов булевых функций предложен Супруном В. П. в [4]. В случае $k \geq 3$ быстрый алгоритм построения полинома по $\bmod k$ для k-значных функций найден Таранниковым Ю. В. В [5] описаны формулы подсчета коэффициентов поляризованных полиномов k-значных функций.

Автором предлагаются формулы для нахождения коэффициентов обобщенно-поляризованных полиномов k-значных функций.

Теорема 1. *Пусть k — простое число, $\delta = (\delta_1, \ldots, \delta_n)$ — обобщенный вектор поляризации,*

в котором $\delta_i = (s_{i,k-1}(x_i), \ldots, s_{i,0}(x_i))$, где

$$s_{i,m}(x_i) = c^i_{m,m} x_i^m + \cdots + c^i_{m,1} x_i + c^i_{m,0},$$

где $c^i_{m,m}, \ldots, c^i_{m,1}, c^i_{m,0} \in E_k$, $c_{m,m} \neq 0$, $m = k-1, \ldots, 1, 0$, $i = 1, \ldots, n$, и $\delta' = (\delta_2, \ldots, \delta_n)$. Пусть $f(x_1, \ldots, x_n) \in P_k$ и $f_i(x_2, \ldots, x_n) = f(i, x_2, \ldots, x_n)$, $i \in E_k$.

Тогда

если $n = 1$, то

$$c^\delta_f(k-1) = \frac{c_f(k-1)}{c^1_{k-1,k-1}},$$

$$c^\delta_f(i) = \frac{1}{c^1_{i,i}} \left(c_f(i) - \sum_{j=i+1}^{k-1} c^1_{j,i} c^\delta_f(j) \right),$$

$i = k-2, \ldots, 1, 0$;

если $n \geq 2$, то

$$c^\delta_f(k-1, x_2, \ldots, x_n) = \frac{c^{\delta'}_f(k-1, x_2, \ldots, x_n)}{c^1_{k-1,k-1}},$$

$$c^\delta_f(i, x_2, \ldots, x_n) = \frac{1}{c^1_{i,i}} \left(c^{\delta'}_f(i, x_2, \ldots, x_n) - \sum_{j=i+1}^{k-1} c^1_{j,i} c^\delta_f(j, x_2, \ldots, x_n) \right),$$

$i = k-2, \ldots, 1, 0$.

По формулам теоремы 1 для k-значной функции $f(x_1, \ldots, x_n)$ коэффициенты $c^\delta_f(\alpha)$, $\alpha \in E^n_k$, ее обобщенно-поляризованного по вектору δ полинома можно быстро найти, если известны коэффициенты $c_f(\alpha)$, $\alpha \in E^n_k$, ее полинома mod k. Коэффициенты полинома по mod k для k-значной функции по ее значениям можно отыскать по формулам, указанным в [5].

Работа поддержана РФФИ, гранты 07-01-00444 и 09-01-00701-а.

Список литературы

1. Яблонский С. В. Введение в дискретную математику. — М.: Наука, 1986.

2. Селезнева С. Н. О сложности задания k-значных функций обобщенно-поляризованными полиномами // Дискретная математика. — 2009. — Т. 21, вып. 4. — С. 20–29.

3. Гаврилов Г. П., Сапоженко А. А. Задачи по дискретной математике. — М.: Наука, 1974.

4. Супрун В. П. Табличный метод полиномиального разложения булевых функций // Кибернетика. — 1987. — № 1. — С. 116–117.

5. Селезнева С. Н., Маркелов Н. К. Быстрый алгоритм построения векторов коэффициентов поляризованных полиномов k-значных функций // Ученые записки Казанского университета. Сер. Физико-математические науки. — 2009. — Т. 151, кн. 2. — С. 147–153.

ОБ ОДНОМ ОБОБЩЕНИИ ЛОГИКИ ЛИНЕЙНОГО ВРЕМЕНИ

Р. В. Хелемендик (Москва)

Логика линейного времени является расширением логики высказываний, в которой наряду с классическими связками добавлены следующие временны́е: $\bigcirc$ (в следующий момент), $\Box$ (всегда), $\Diamond$ (в некоторый момент), U (до тех пор, пока). Традиционно моделью для формулы называется бесконечная последовательность (возможно повторяющихся) вершин с выделенной начальной вершиной, в которой эта формула истинна. Формула называется выполнимой, если она истинна в некоторой модели. В настоящей работе предложено обобщение логики линейного времени, в котором наряду с бесконечными моделями рассматриваются также и конечные. Модифицирована система аксиом, установлена ее корректность и полнота — с помощью авторского алгоритма вывода общезначимых формул из аксиом, отличного от переборного. Выделена специальная формула Ψ такая, что выполнимость произвольной формулы Θ в традиционной логике линейного времени равносильна выполнимости формулы $(\Theta \wedge \Psi)$ в обобщённой, и вместе с тем даны примеры формул, выполнимых в обобщённой логике линейного времени и невыполнимых в традиционной.

Основные определения. Каждая пропозициональная переменная есть *формула*. Если φ и ψ *формулы*, то θ, являющаяся одним из 9 выражений: $\top$, $\neg\varphi$, $(\varphi \vee \psi)$, $(\varphi \wedge \psi)$, $(\varphi \to \psi)$, $\bigcirc\varphi$, $\Box\varphi$, $\Diamond\varphi$, $(\varphi\ U\ \psi)$ тоже называется является *формулой*. Других *формул* нет.

Моделью будем называть пару $M = \langle N, L\rangle$, где N — связный ориентированный граф с выделенной вершиной u_0, каждая вершина

которого имеет не более одного сына, а L — функция означивания, сопоставляющая каждой вершине множество пропозициональных переменных. *Полным путём* в графе называется бесконечный путь или цепь, последняя вершина которой не имеет сыновей.

Истинность формулы θ в вершине u_i модели M (обозначим это $M, u_i \models \theta$) определяется индуктивно.

— Если $\theta = \top$, то $M, u_i \models \theta$.

— Если $\theta = p$, то $M, u_i \models \theta \rightleftharpoons p \in L(u_i)$.

— Если $\theta = \neg\varphi$, то $M, u_i \models \theta \rightleftharpoons M, u_i \not\models \varphi$ (неверно $M, u_i \models \varphi$).

— Если $\theta = (\varphi \wedge \psi)$, то $M, u_i \models \theta \rightleftharpoons (M, u_i \models \varphi$ и $M, u_i \models \psi)$.

— Если $\theta = (\varphi \vee \psi)$, то $M, u_i \models \theta \rightleftharpoons (M, u_i \models \varphi$ или $M, u_i \models \psi)$.

— Если $\theta = (\varphi \to \psi)$, то $M, u_i \models \theta \rightleftharpoons (M, u_i \not\models \varphi$ или $M, u_i \models \psi)$.

— Если $\theta = \bigcirc\varphi$, то $M, u_i \models \theta \rightleftharpoons M, u_j \models \varphi$ для сына u_j вершины u_i, либо вершина u_i не имеет сына.

— Если $\theta = \Box\varphi$, то $M, u_i \models \theta \rightleftharpoons$ для полного пути с началом в вершине u_i в каждой его вершине u_j верно $M, u_j \models \varphi$.

— Если $\theta = \Diamond\varphi$, то $M, u_i \models \theta \rightleftharpoons$ для полного пути с началом в вершине u_i существует вершина u_j, для которой верно $M, u_j \models \varphi$.

— Если $\theta = (\varphi\, U\, \psi)$, то $M, u_i \models \theta \rightleftharpoons$ для полного пути с началом в вершине u_i существует вершина u_j, для которой верно $M, u_j \models \psi$, а в каждой вершине u_k этого пути, предшествующей u_j, верно $M, u_j \models \varphi$.

Формула θ *истинна в модели* M, если она истинна в выделенной вершине u_0 этой модели. Формула θ *выполнима*, если она истинна в некоторой модели. Формула θ *общезначима*, если она истинна в каждой модели. В дальнейшем положим $\bot \rightleftharpoons \neg\top$, $\varphi \equiv \psi \rightleftharpoons ((\varphi \to \psi) \wedge (\psi \to \varphi))$.

Отметим, что традиционно (см. [1]) модель M мыслится как бесконечная, поэтому считается, что $M, u_i \models \bigcirc\varphi \rightleftharpoons M, u_j \models \varphi$ для сына u_j вершины u_i. Для моделирования конечности модели в указанной работе предлагается введение специальной формулы и бесконечного числа повторяющихся вершин. Однако, как будет показано ниже, класс выполнимых формул с традиционной семантикой с бесконечными моделями уже, нежели класс выполнимых формул с обобщённой.

Введём следующую *систему аксиом* (схем аксиом) и *правил вывода*:

(Ax1) корректная и полная система аксиом логики высказываний,

(Ax2) $\Diamond\varphi \equiv (\top\, U\, \varphi)$, (Ax3) $\Box\varphi \equiv \neg\Diamond\neg\varphi$,

(Ax4) $\bigcirc(\varphi \vee \psi) \equiv (\bigcirc\varphi \vee \bigcirc\psi)$, (Ax5) $(\bigcirc\varphi \wedge \neg\bigcirc\bot) \equiv \neg\bigcirc\neg\varphi$,

(Ax6) $(\varphi\ U\ \psi) \equiv (\psi \vee ((\varphi \wedge \bigcirc(\varphi\ U\ \psi)) \wedge \neg\bigcirc\bot))$,
(R1) $(\varphi \to \psi),\ \varphi \vdash \psi$, (R2) $(\varphi \to \psi) \vdash (\bigcirc\varphi \to \bigcirc\psi)$,
(R3) $(\varphi_1 \to (\neg\varphi_2 \wedge \bigcirc\varphi_1)) \vdash (\varphi_1 \to \neg(\psi\ U\ \varphi_2))$.

Из данной системы аксиом и правил вывода выводимы следующие аксиомы и правило вывода: $(\Box(\varphi \to \psi) \to (\Box\varphi \to \Box\psi))$, $(\bigcirc(\varphi \to \psi) \to (\bigcirc\varphi \to \bigcirc\psi))$, $\Box\varphi \equiv (\varphi \wedge \bigcirc\Box\varphi)$, $(\Box(\varphi \to \bigcirc\varphi) \to (\varphi \to \Box\varphi))$, $((\varphi\ U\ \psi) \to \Diamond\psi)$, $\varphi \vdash \Box\varphi$. В то же время прежние аксиомы $\bigcirc\varphi \equiv \neg\bigcirc\neg\varphi$, $(\varphi\ U\ \psi) \equiv (\psi \vee \bigcirc(\varphi\ U\ \psi))$ не являются выводимыми, так как не являются общезначимыми формулами.

Корректность и полнота системы аксиом. Корректность введённой системы аксиом и правил вывода доказывается прямой проверкой, т. е. установлением общезначимости данных формул и сохранением общезначимости в правилах вывода. Полноту системы аксиом докажем с помощью алгоритма распознавания выполнимости формул логики линейного времени и алгоритма вывода общезначимых формул из аксиом, полученных по соответствующим алгоритмам из работы [2]. В алгоритме распознавания выполнимости изменяются правило эквивалентности, правило завершения, правило новых вершин. В алгоритме построения выводов общезначимых формул из аксиом строятся новые выводы аналогов вспомогательных аксиом и правил вывода, из аксиом (Ax1)–(Ax6) и правил (R1)–(R3). Имеют место следующие теоремы.

Теорема 1. *Если формула* Θ *выводима, то она общезначима.*

Теорема 2. *Если формула* Θ *общезначима, то она выводима.*

Сравнение с традиционной семантикой. Положим $\Psi = \Box\neg\bigcirc\bot$. Имеет место следующая теорема.

Теорема 3. *Формула* Θ *выполнима в традиционной семантике тогда и только тогда, когда формула* $(\Theta \wedge \Psi)$ *выполнима в обобщённой.*

Таким образом, обобщенная семантика логики линейного времени сохраняет в себе все свойства традиционной. В то же время существуют примеры и классы формул, выполнимых в обобщённой семантике, и не выполнимых в традиционной. Например, формулы $(\bigcirc\varphi \wedge \bigcirc\neg\varphi)$ и $((\varphi \vee \bigcirc\Diamond\varphi) \wedge \neg\Diamond\varphi)$ истинны в модели, состоящей из единственной вершины, не имеющей сыновей.

Работа выполнена при финансовой поддержке программы фундаментальных исследований Отделения математических наук РАН “Алгебраические и комбинаторные методы математической кибернетики и информационные системы нового поколения”.

Список литературы

1. Emerson E. A. Temporal and modal logic // Handbook of Theoretical Computer Science. V. B. — Elsevier and The MiT Press, 1990. —

Р. 995–1072.
2. Хелемендик Р. В. Алгоритм распознавания выполнимости формул логики ветвящегося времени и эффективный алгоритм построения выводов общезначимых формул из аксиом // Математические вопросы кибернетики. Вып. 15. — М.: Физматлит, 2006. — С. 217–266.

О БЕСПОВТОРНЫХ БУЛЕВЫХ ФУНКЦИЯХ В ОДНОМ ПРЕДЭЛЕМЕНТАРНОМ БАЗИСЕ

И. К. Шаранхаев (Улан-Удэ)

Под *базисом* понимаем конечную полную систему булевых функций, содержащую константы.

Терм Φ над базисом B называется *бесповторным*, если каждая переменная входит в него не более одного раза.

Булева функция f называется *бесповторной* в базисе B, если существует бесповторный терм Φ над B, представляющий функцию f. В противном случае f называется *повторной* в B.

Функция f называется *слабоповторной* в базисе B, если любая остаточная функция от функции f является бесповторной, а сама f повторна в базисе B.

Базис $B_0 = \{\vee,\ \cdot,\ -,\ 0,\ 1\}$ называется *элементарным*, а базис $B_0 \cup \{f\}$, где f слабоповторна в B_0, называется *предэлементарным*.

Ниже предлагается необходимое и достаточное условие бесповторности булевых функций в одном предэлементарном базисе.

Все неопределяемые понятия можно найти, например, в [1].

Будут использоваться следующие обозначения:

– символом $\tilde{x}$ обозначается набор $(x_1, \ldots, x_n)$;

– rang f — ранг функции f;

– $\rho(f)$ — множество всех существенных переменных функции f;

– $\delta(f)$ — множество всех фиктивных переменных функции f.

Назовем переменную x_i функции f *фиктивной*, если $f^0_{x_i} = f^1_{x_i}$ и *существенной* в противном случае.

Рангом функции f называется число ее существенных переменных.

Будем говорить, что функции f и g *связаны отношением* $\preceq$, и писать $f \preceq g$, если для любого набора $\tilde{\sigma}$ выполняется $f(\tilde{\sigma}) \leq g(\tilde{\sigma})$.

Функция f называется *обобщенно монотонной по переменной* x, если выполняется либо $f^0_x \preceq f^1_x$, либо $f^0_x \succeq f^1_x$. Для краткости записи обобщенную монотонность функции f по переменной x будем обозначать так: $f \in M_x$.

Производной функции $f(x_1, \ldots, x_n)$ по переменной x_i называется функция $f'_{x_i} = \dfrac{\partial f}{\partial x_i} = f^0_{x_i} \oplus f^1_{x_i}$.

Понятие производной функции по переменной распространяется индуктивно на множество переменных следующим образом:

$$\frac{\partial f}{\partial x_{i_1} \ldots \partial x_{i_s}} = \frac{\partial \left(\dfrac{\partial f}{\partial x_{i_1} \ldots \partial x_{i_{s-1}}} \right)}{\partial x_{i_s}}.$$

Функцию f будем называть *неустойчивой*, если либо $\operatorname{rang} f < 2$, либо для любого $x \in \rho(f)$ справедливо включение $f \in M_x$ и выполняется одно из условий:

(1) для некоторой константы σ справедливы $\delta(f) \subset \delta(f^\sigma_x)$ и $\delta(f) = \delta(f^{\bar\sigma}_x)$, причем если $\delta(f^\sigma_x) \setminus \delta(f) = \{y\}$, то не выполняется равенство $\delta(f) = \delta(f^0_y) = \delta(f^1_y)$;

(2) $\delta(f) = \delta(f^0_x) = \delta(f^1_x)$ и $\delta(f) \subset \delta(f'_x)$;

(3) $\delta(f) \subset \delta(f^0_x)$, $\delta(f) \subset \delta(f^1_x)$ и найдется переменная $y \in \rho(f'_x)$ такая, что $\delta(f'_x) \subset \delta((f'_x)'_y)$.

Функцию f будем называть *наследственно неустойчивой*, если сама f и все ее остаточные функции являются неустойчивыми.

Автором доказана следующая

Теорема. *Функция f бесповторна в базисе $\{\vee, \cdot, -, 0, 1, x_1(x_2 \vee x_3) \vee x_3 x_4\}$ тогда и только тогда, когда она является наследственно неустойчивой.*

Список литературы

1. Перязев Н. А. Основы теории булевых функций. — М.: Физматлит, 1999.

О ПЕРИОДИЧНОСТИ ЗНАЧЕНИЙ СЛУЧАЙНЫХ ВЫРАЖЕНИЙ В КВАЗИГРУППАХ

А. Д. Яшунский (Москва)

Рассмотрим однородные по времени цепи Маркова с множеством состояний $Q = \{1, 2, \ldots, q\}$, начальным распределением $\{\pi_i\}$ и матрицей переходов $\{p_{ij}\}$ (см. [3]). Пусть $p^{(n)}_{ij}$ — вероятность перехода из состояния i в состояние j за n шагов. Состояние j *достижимо* из состояния i, если $\exists n : p^{(n)}_{ij} > 0$. Состояния i и j *сообщаются*, если

они достижимы друг из друга. Цепь Маркова *неразложима*, если любые два её состояния сообщаются. *Периодом* состояния i назовём $d(i) = \text{НОД}\{n : p_{ii}^{(n)} > 0\}$. Состояние i *периодическое*, если $d(i) > 1$.

Теорема 1 [3]. *У неразложимой цепи Маркова все $d(i)$ совпадают.*

Построим по цепи Маркова систему автоматных языков (подробнее о языках см. [2]), и в её терминах определим понятия неразложимости и периодичности, эквивалентные соответствующим понятиям для цепи Маркова.

Введём алфавиты $F = \{f_1, \ldots, f_q\}$ и $S = \{S_1, \ldots, S_q\}$. В качестве терминалов грамматики используем алфавит $Q \cup F$, а в качестве нетерминалов — алфавит S. Определим множество правил $R = \{S_i \to i : \pi_i > 0\} \cup \{S_j \to f_j S_i : p_{ij} > 0\}$.

Множество правил R *неразложимо*, если в нём любые два нетерминала связаны цепочкой вывода. Легко проверить

Утверждение 1. *Цепь Маркова неразложима тогда и только тогда, когда неразложимо соответствующее множество правил.*

Пусть язык L_i порождается грамматикой с начальным символом S_i и множеством правил R. Из построения множества R вытекает

Утверждение 2. *Если R неразложимо, то все L_i непустые.*

Обозначим через $|w|$ длину проекции (рассмотрение именно проекции обусловлено дальнейшими обобщениями конструкции; для цепей Маркова можно также рассматривать просто длину слова) слова w на множество F. *Периодом* языка L назовём $d(L) = \text{НОД}\{|w_2| - |w_1| : w_1, w_2 \in L\}$. Если $d(L) > 1$, то язык L *периодический*. Содержательно, периодичность языка L означает, что в него входят только слова w, у которых $|w|$ принадлежит некоторой арифметической прогрессии с разностью $d(L)$. В силу равенства $d(L_i) = d(i)$, аналогично теореме 1, верно:

Утверждение 3. *Если R неразложимо, то все $d(L_i)$ совпадают.*

Определим периодичность для языков, порождаемых алгебраическими системами. Под *алгебраической системой* будем понимать множество $Q = \{1, \ldots, q\}$, множество 0-арных операций $N \subseteq Q$ (*носитель*) и конечное множество операций $F = \{f_k\}$, арности 1 и выше.

По алгебраической системе построим систему контекстно-свободных (КС) языков. В качестве терминалов возьмём $Q \cup F$, а в качестве нетерминалов $S = \{S_1, \ldots, S_q\}$. Определим множество правил $R = \{S_i \to i : i \in N\} \cup \{S_i \to f_k S_{i_1} \ldots S_{i_m} : f_k(i_1, \ldots, i_m) = i\}$. Пусть язык L_i порождается R с начальным символом S_i. Слова из L_i в точности соответствуют выражениям со значением $i \in Q$. Рассмо-

тренный выше случай автоматных языков фактически описывает системы, у которых в F есть только унарные операции.

Для *неразложимости* R и *периода* языка сохраняются данные выше определения. Отметим, что для КС-языков утверждение 2, вообще говоря, не верно. В частности, для системы с $Q = \{0, 1\}$, $N = \{0\}$ и $F = \{\oplus\}$ множество правил $R = \{S_0 \to \oplus S_0 S_0, S_1 \to \oplus S_0 S_1, S_1 \to \oplus S_1 S_0, S_0 \to \oplus S_1 S_1, S_0 \to 0\}$ неразложимо, но язык L_1 пустой. Утверждение 3 обобщается в

Утверждение 4. *Если R неразложимо и все L_i непустые, то все L_i имеют один и тот же период.*

Непустота всех языков L_i равносильна тому, что замыкание носителя N относительно операций из F совпадает с Q.

Рассмотрим периодичности, возникающие в квазигрупповых системах. Бинарная операция $\cdot$ на множестве Q *квазигрупповая*, если уравнения $a = x \cdot b$ и $a = b \cdot y$ всегда однозначно разрешимы относительно x и y [1]. Далее *квазигруппой* называется система с $F = \{\cdot\}$.

Теорема 2. *Пусть языки $L_1, L_2, \ldots, L_q$ построены по квазигруппе Q с носителем N и все $L_i \neq \emptyset$. Языки L_i периодические тогда, и только тогда, когда существует гомоморфизм φ квазигруппы Q в группу $\mathbb{Z}_r$ такой, что $N \subseteq \varphi^{-1}(1)$.*

Доказательство. Необходимость. Неразложимость множества правил легко следует из свойств квазигруппового умножения. Если все языки L_i периодические, то по утверждению 4 они имеют общий период $r > 1$. Пусть $\varphi(i) = (|w| + 1) \bmod r$, где w некоторое слово из L_i. $\varphi(i)$ не зависит от выбора w в силу $d(L_i) = r$. Проверим, что φ — гомоморфизм: пусть $w_i \in L_i, w_j \in L_j$ и $i \cdot j = k$, тогда $\cdot w_i w_j \in L_k$; $\varphi(k) = (|\cdot w_i w_j| + 1) \bmod r = (1 + |w_i| + |w_j| + 1) \bmod r = \varphi(i) + \varphi(j)$. При $w = m \in N$: $|w| = 0$, откуда $\varphi(m) = 1$.

Достаточность. Пусть задан гомоморфизм φ квазигруппы Q в группу $\mathbb{Z}_r$ такой, что $N \subseteq \varphi^{-1}(1)$. Покажем, что для любого i и любого $w \in L_i$ имеет место $(|w| + 1) \bmod r = \varphi(i)$. Проведём индукцию по значениям $|w|$. Для $|w| = 0$: $w = m \in N$, следовательно, $1 = \varphi(m)$, и утверждение верно. Пусть утверждение верно для всех $|w| < n$, рассмотрим $w \in L_k$, $|w| = n$. Очевидно, $w = \cdot w_i w_j$ для некоторых $w_i \in L_i$, $w_j \in L_j$, где $k = i \cdot j$, причём для w_i и w_j выполнено предположение индукции. Тогда $(|\cdot w_i w_j| + 1) \bmod r = (|w_i| + 1) \bmod r + (|w_j| + 1) \bmod r = \varphi(i) + \varphi(j) = \varphi(i \cdot j) = \varphi(k)$, что доказывает шаг индукции. Следовательно, для каждого i язык L_i периодический и r является делителем $d(L_i)$. Теорема доказана.

Теорема 2 обобщает критерий периодичности случайных блу-

жданий в группе [5] на случай квазигрупп. Вместе с результатами из [4] теорема 2 характеризует предельное поведение значений случайных выражений в квазигруппах: если Q — квазигруппа с носителем N и Q' — замыкание N по умножению, то выражения со значениями из $Q \setminus Q'$ имеют вероятность 0, а со значениями в Q' — либо в пределе равномерно распределены, либо образуют периодические языки и не имеют предельного распределения.

Автор выражает благодарность О.М. Касим-Заде за полезные обсуждения и внимание к работе.

Работа выполнена при финансовой поддержке РФФИ (проект 08–01–00863), программы поддержки ведущих научных школ РФ (проект НШ–4437.2010.1) и программы фундаментальных исследований ОМН РАН «Алгебраические и комбинаторные методы математической кибернетики и информационные системы нового поколения».

Список литературы

1. Белоусов В. Д. Основы теории квазигрупп и луп. — М.: Наука, 1967.

2. Гросс М., Лантен А. Теория формальных языков и грамматик. — М.: Мир, 1971.

3. Феллер В. Введение в теорию вероятностей и ее приложения. — М.: Мир, 1984.

4. Яшунский А. Д. О предельных вероятностях значений случайных выражений в квазигруппах // Мат-лы XVIII международной школы-семинара "Синтез и сложность управляющих систем" им. академика О. Б. Лупанова. — М.: Изд-во мех-мат ф-та МГУ, 2009. — С. 128–132.

5. Saloff-Coste L. Random walks on finite groups. Probability on discrete structures // Enc. Math. Sci. — Springer, Berlin, 2004. — 110. — P. 263–346.

Секция «Комбинаторный анализ и теория графов»

Подсекция «Комбинаторный анализ»

ДВА ТИПА r-ПЕРЕСТАНОВОК И r-МНОГОЧЛЕНЫ ЭЙЛЕРА

Л. Н. Бондаренко (Пенза), М. Л. Шарапова (Москва)

Для слов $\sigma=\sigma_1\dots\sigma_n$ над алфавитом $[n]=\{1,\dots,n\}$ из симметрической группы S_n определим, следуя Фоата [1], функцию (статистику) $\mathrm{RISE}(\sigma)=|\{i:\sigma_i<\sigma_{i+1}, 0\le i\le n-1, \sigma_0=0\}|$, означающую число подъемов перестановки $\sigma\in S_n$.

Числа $A_{n,k}=|\{\sigma:\sigma\in S_n, \mathrm{RISE}(\sigma)=k\}|$ называются числами Эйлера. Они удовлетворяют следующему рекуррентному соотношению $A_{0,k}=\delta_{0,k}, A_{n,k}=kA_{n-1,k}+(n-k+1)A_{n-1,k-1}, n\in\mathbf{N}, k\in\mathbf{Z}$, где $\delta_{i,j}$ — символ Кронекера, а статистика W также называется эйлеровой, если $A_{n,k}=|\{\sigma:\sigma\in S_n, W(\sigma)=k\}|$, $k=1,\dots,n$ [1].

Если для всех $\sigma\in S_n$ имеем $W(\sigma)+\overline{W}(\sigma)=n+1$, то статистики W и $\overline{W}$ назовем дополнительными. Очевидно, что $\overline{\overline{W}}(\sigma)=W(\sigma)$, а RISE дополнительна статистике $\mathrm{DES}(\sigma)=|\{i:\sigma_i>\sigma_{i+1}, 1\le i\le n, \sigma_{n+1}=0\}|$ — число спусков перестановки $\sigma\in S_n$.

Для многочлена Эйлера $A_n(t)=\sum_{k=1}^{n}A_{n,k}t^k$, служащего производящей функцией чисел $A_{n,k}$, справедлива рекуррентная формула $A_0(t)=1$, $A_n(t)=ntA_{n-1}(t)+t(1-t)A'_{n-1}(t)$, $n\in\mathbf{N}$, из которой следует, что $A_n(t)=t^{n+1}A_n(t^{-1})$. Поэтому эйлеровость статистики W влечет эйлеровость $\overline{W}$. Отметим также, что нормированные многочлены $P_n(t)=A_n(t)/A_n(1)$ позволяют найти асимптотику распределения $\{A_{n,k}/n!\}_{k=1}^{n}$ при $n\to\infty$ [2].

Код Лемера $\xi=L(\sigma)$ перестановки $\sigma\in S_n$ есть слово $\xi=\xi_1\dots\xi_n$ над алфавитом $\{0,\dots,n-1\}$, в котором $\xi_i=|\{j:\sigma_j<\sigma_i, 1\le j\le i-1\}|$. С по-

мощью функции IMA(ξ) (число различных букв в слове ξ) определяется эйлерова статистика IMAL(σ)=IMA(ξ) перестановки $\sigma\in S_n$, причем функция IMA позволяет получить и другие эйлеровы статистики [1]. Статистика ILAL(σ)=ILA(ξ), где ILA(ξ) — число букв в алфавите $[n]$, отсутствующих в слове ξ, также является эйлеровой, так как она дополнительна к IMAL(σ).

Фиксируя ключ $\kappa\in S_n$, определим код $\tau=VP(\sigma,\kappa)$ перестановки $\sigma\in S_n$ словом $\tau=\tau_1\dots\tau_n$ над алфавитом $[n]$, где $\tau_i=\sigma_i+\kappa_i(\mathrm{mod}\ n)$ — наименьшие положительные вычеты. Функция IVP(σ)=$n^{-1}\sum_{i=1}^{n}\tau_i$ для любого $\kappa\in S_n$ эйлерова [3], как и дополнительная к ней функция EXC(σ)=$\sum_{i=1}^{n}\bar{\tau}_i$, где $\bar{\tau}_i$=1, если $\sigma_i+\kappa_i>n$, и $\bar{\tau}_i$=0, если $\sigma_i+\kappa_i\le n$.

Авторами найдена биекция $\Phi: S_n\to S_n$, позволяющая записать IMAL(σ)=EXC($\Phi(\sigma)$), что дополняет результаты работы [1].

IMA(τ) задает статистику IMAVP(σ)=IMA(τ), не являющуюся эйлеровой. Для IMAVP найдено асимптотическое распределение, а также при нечетном n и фиксированном ключе $\kappa\in S_n$ решена задача о "хороших" перестановках: $|\{\sigma:\sigma\in S_n,\mathrm{IMAVP}(\sigma)=n\}|\sim n!^2/n^n$ [2].

Статистики RISE, IMAL естественным образом обобщаются на множество всех перестановок σ мультимножества $\{i^{m_i}\}_{i=1}^{n}$, где m_i — кратность i. Они имеют одинаковые распределения и являются обобщенными эйлеровыми статистиками. Для ключа $\kappa=\kappa_1^{m_1}\dots\kappa_n^{m_n}$, где $\kappa_i=n-i$ для $1\le i\le n-1$, а $\kappa_n=n$, в [3] доказана эйлеровость обобщенной статистики IVP$_0$(σ)=$1+n^{-1}\sum_{i=1}^{m}\tau_i$, причем $m=m_1+\dots+m_n$, а $\tau_i=\sigma_i+\kappa_i(\mathrm{mod}\ n)$ — наименьшие неотрицательные вычеты.

Определение 1. *Пусть $S_{n,r}$ — множество всех перестановок мультимножества $\{i^r\}_{i=1}^{n}$. Тогда перестановка $\sigma\in U_{n,r}, U_{n,r}\subseteq S_{n,r}$ называется r-перестановкой* I *типа, если все числа между двумя встречающимися i в $\sigma\in U_{n,r}$ не меньше этого i. Полагаем $U_{n,1}=S_{n,1}$.*

Определение 2. *Перестановка $\sigma\in V_{n,r}, V_{n,r}\subseteq S_{rn}$ называется r-перестановкой* II *типа, если для нее выполнены следующие условия:* 1)$\sigma_{r(i-1)+1}<\sigma_{r(i-1)+2}<\dots<\sigma_{ri}$, *где* $i=1,\dots,n$, *и* 2)$\sigma_{ri-1}<\sigma_{ri+1}$, *где* $i=1,\dots,n-1$. *Полагаем $V_{n,1}=S_n$.*

Отметим, что r-перестановки из $U_{n,r}$ и $V_{n,r}$ имеют степень rn, причем, как будет показано ниже, $|U_{n,r}|=|V_{n,r}|$. Поэтому представляет интерес сравнение статистик для двух типов r-перестановок.

Теорема 1. *r-числа Эйлера $A_{n,r,k}=|\{\sigma:\sigma\in U_{n,r},\mathrm{RISE}(\sigma)=k\}|$ типа* I, *где $k=1,\dots,n$, удовлетворяют при $n\in\mathbf{N}, k\in\mathbf{Z}$ соотношению*

$$A_{0,r,k}=\delta_{0,k}, A_{n,r,k}=kA_{n-1,r,k}+(r(n-1)-k+2)A_{n-1,r,k-1}. \quad (1)$$

Теорема 2. *r-числа Эйлера* $\hat{A}_{n,r,k}=|\{\sigma : \sigma\in V_{n,r}, \mathrm{DES}(\sigma)=k\}|$ *типа* II, *где* $k=1,\ldots,n$, *удовлетворяют при* $r\geq 2$ *соотношению*

$$\hat{A}_{1,r,k}=\delta_{1,k},\ \hat{A}_{n,r,k}=\hat{A}_{n-1,r,k}+r(n-1)\hat{A}_{n-1,r,k-1},\ n\geq 2,\ k\in\mathbf{Z}. \quad (2)$$

В теоремах 1 и 2 параметр r определяет род чисел Эйлера, а доказательство выражений (1) и (2) проводится методом математической индукции по n при фиксированном r. Для r-многочленов Эйлера $A_{n,r}(t)=\sum_{k=1}^{n} A_{n,r,k}t^k$ и $\hat{A}_{n,r}(t)=\sum_{k=1}^{n}\hat{A}_{n,r,k}t^k$ с помощью выражений (1) и (2) находятся рекуррентные формулы $A_{0,r}(t)=1$, $A_{n,r}(t)=(r(n-1)+1)tA_{n-1,r}(t)+t(1-t)A'_{n-1,r}(t)$, $n\geq 1$ и $\hat{A}_{1,r}(t)=t$, $\hat{A}_{n,r}(t)=(r(n-1)t+1)\hat{A}_{n-1,r}(t), n\geq 2, r\geq 2$, из которых при $t=1$ получаем равенство $A_{n,r}(1)=\hat{A}_{n,r}(1)$, т. е. $|U_{n,r}|=|V_{n,r}|$.

Теорема 3. $A_{n,r,k}=|\{\sigma : \sigma\in U_{n,r}, \mathrm{IMAL}(\sigma)=k\}|$, *где* $k=1,\ldots,n$, $A_{n,r,k}=|\{\sigma : \sigma\in V_{n,r}, \mathrm{ILAL}(\sigma)=k\}|$, *где* $k=1,\ldots,n$.

Доказательство теоремы 3 проводится индукцией по n при фиксированном r с использованием соотношения (1).

В [4] для нормированных многочленов $P_{n,r}(t)=A_{n,r}(t)/A_{n,r}(1)$ получена асимптотика распределения их коэффициентов. Аналогично для многочленов $\hat{P}_{n,r}(t)=\hat{A}_{n,r}(t)/\hat{A}_{n,r}(1)$ справедлива

Теорема 4. *При* $r\geq 2$ *распределение коэффициентов многочленов* $\hat{P}_{n,r}(t)$ *асимптотически нормально с математическим ожиданием* $\hat{\mu}_{n,r}=n-\ln n/r+O(1)$ *и дисперсией* $\hat{\sigma}^2_{n,r}=\ln n/r+O(1)$.

Функция $\mathrm{IVP}_0(\sigma)=1+n^{-1}\sum_{i=1}^{rn}\tau_i$, где $\tau_i=\sigma_1+\kappa_i(\mathrm{mod}\ n)$ — наименьшие неотрицательные вычеты, $\sigma\in U_{n,r}$ или $\sigma\in V_{n,r}$, требует дополнительного изучения для различных ключей κ.

Работа выполнена при финансовой поддержке РГНФ (проект 09-06-28615 а/В).

Список литературы

1. Фоата Д. Распределения типа Эйлера и Макмагона на группе перестановок // Проблемы комбинаторного анализа: сб. статей. — М.: Мир, 1980. — С. 120–141.

2. Бондаренко Л. Н., Шарапова М. Л. Статистики на классах отображений // Дискретные модели в теории управляющих систем: VIII Международная конференция (Москва, 6–9 апреля 2009 г.). Труды. — М.: Издательский отдел факультета ВМиК МГУ им. М. В. Ломоносова; МАКС Пресс, 2009. — С. 33–39.

3. Бондаренко Л. Н. О статистиках Эйлера на группе перестановок // Материалы IX Международного семинара "Дискретная ма-

тематика и ее приложения" (Москва, МГУ, 18–23 июня 2007 г.). — М.: Изд-во механико-математического факультета МГУ, 2007. — С. 206–208.

4. Бондаренко Л. Н. Многочлены Эйлера и их связь с перманентами и гафнианами // Материалы XVIII Международной школы-семинара "Синтез и сложность управляющих систем" имени академика О. Б. Лупанова (Пенза, 28 сентября — 3 октября 2009 г.). — М.: Изд-во механико-математического факультета МГУ, 2009. — С. 13–18.

К ВОПРОСУ О РЕШЕТКЕ МУЛЬТИМНОЖЕСТВ

Д. Б. Буй, Ю. А. Богатырёва (Киев)

Существует широкий класс задач, особенностью которых являются множественность и повторяемость данных; для их решения математической моделью выступают мультимножества (обширная библиография и исторический обзор приведены в [1–3]).

Одним из наиболее естественных применений является применение мультимножеств в табличных базах данных [4–7].

Мультимножества также используются в декларативных языках программирования [8] и спецификаций [9]. Д. Кнут использует мультимножества в контекстно-свободных мультиязыках [10].

Мультимножества также применяются в теории сетей Петри [11], для распознавания символов, для представления и кодирования информации. Кроме компьютерных наук мультимножества используются в λ-исчислении [12], физике, философии, логике, лингвистике [1, 13], в вычислениях на ДНК [14].

Несмотря на достаточно широкое практическое применение, собственно теории мультимножеств посвящено относительно мало работ [3, 15].

Естественно, столь широкое практическое применение вызывает необходимость в дальнейшем развитии математической теории мультимножеств.

Доклад посвящен частному вопросу — решетке мультимножеств, что поясняет структуру семейства мультимножеств. Формально *мультимножество* α *с основой* U — функция вида $\alpha\colon U \to N^+$, где U — множество в класическом канторовском понимании, а N^+ — множество натуральных чисел без нуля [3, 6].

Характеристическая функция мультимножества задается кусочной схемой вида

$$\chi_A(d) = \begin{cases} \alpha(d), \text{ если } d \in dom\alpha, \\ 0, \text{ иначе;} \end{cases}$$

для всех $d \in D$, где D — универсум элементов основ мультимножеств [3, 6]. Очевидно, что по характеристической функции соответствующее мультимножество восстанавливается однозначно.

Введем бинарное отношение включения. Мультимножество β *включается* в мультимножество α ($\beta \preccurlyeq \alpha$), если для их характеристических функций выполняется $\chi_\beta(d) \leqslant \chi_\alpha(d)$, $\forall d \in D$. Непосредственно проверяется, что введенное отношение является частичным порядком.

Аналоги стандартных теоретико-множественных операций определяются и над мультимножествами: объединение, пересечение, разность, симметрическая разность, дополнение и прямое произведение. Кроме этого имеется ряд операции, отражающих специфику мультимножеств и не имеющих прямых аналогов среди операций над множествами. Это операции сложения, произведения и умножение числа на мультимножество.

Дадим определение операций объединения и пересечения мультимножеств. Операция $\bigcup_{All}$ мультимножествам α и β сопоставляет мультимножество, значение характеристической функции которого на произвольном аргументе d задается как $\max(\chi_\alpha(d), \chi_\beta(d))$. Операция $\bigcap_{All}$ мультимножествам α и β сопоставляет мультимножество, значение характеристической функции которого на произвольном аргументе d задается как $\min(\chi_\alpha(d), \chi_\beta(d))$.

Операции объединения и пересечения мультимножеств имеют стандартные свойства.

Лемма. *Операции* $\bigcup_{All}$ *и* $\bigcap_{All}$ *идемпотентны, коммутативны и ассоциативны.*

Таким образом, можно рассматривать две коммутативные идемпотентные полугруппы: $\langle A, \bigcup_{All}\rangle$ и $\langle A, \bigcup_{All}\rangle$, где A — семейство мультимножеств соответствующего универсума D.

Используя хорошо известный результат теории решеток (см., например, [16]), полугруппа по объединению индуцирует верхнюю полурешетку, а полугруппа по пересечению — нижнюю. Частичные порядки верхней и нижней полурешеток задаются стандартно: $\alpha \leq \beta \Leftrightarrow \alpha \bigcup_{All} \beta = \beta$, $\alpha \lesssim \beta \Leftrightarrow \alpha \bigcap_{All} \beta = \alpha$, причем $\sup_{\leq}(\alpha, \beta) = \alpha \bigcup_{All} \beta$, $\inf_{\lesssim}(\alpha, \beta) = \alpha \bigcap_{All} \beta$.

Непосредственно проверятся, что эти порядки совпадают с порядком включения мультимножеств $\preccurlyeq$. Таким образом, семейство

мультимножеств A с частичным порядком $\preccurlyeq$ является решеткой.

Такой способ построения решетки мультимножеств явно не использовал законы поглощения. Нетрудно показать в общем случае, что порядки верхней и нижней полурешеток совпадают тогда и только тогда, когда выполняются законы поглощения.

Список литературы

1. Blizard W. The development of multiset theory // Notre Dame J. of Formal Logic. — 1989. — V. 30, № 1. — P. 36–66.

2. Кнут Д. Искусство программирования. — М.: Вильямс, 2000.

3. Петровський А. Б. Основные понятия теории мультимножеств. — М.: "Эдиториал УРСС", 2002.

4. Libkin L., Wong L. Query language for bags and aggregates function // J. of Computer and System Sciences. — 1997. — V. 55, № 1. — P. 241–272.

5. Ross K., Stoyanovich J. Symmetric relations and cardinality-bounded multisets in database systems // VLDE, Aug. 31 – Sep 03, Canada, 2004. — V. 30. — P. 912–923.

6. Редько В. Н., Брона Ю. Й., Буй Д. Б., Поляков С. А. Реляційні бази даних: табличні алгебри та SQL-подібні мови. — Київ: "Академперіодика", 2001.

7. Lamperti G., Melchiori M., Zanella M. On multisets in database systems // Multiset Processing, number 2235 in Lecture Notes in CS. — Berlin: Springer-Verlag, 2001. — P. 147–215.

8. Lloyd J. Programming with multisets // Department of Computer Science, University of Bristol, 1998.

9. Кузнецов С. Д. Концептуальное проектирование реляционных баз данных с использованием языка UML [Электронный ресурс].

10. Knuth D. Context-free multilanguages // Theoretical Studies in CS. — Academic Press, 1992. — P. 1–13.

11. Башкин В. А., Ломазова И. А. Подобие обобщенных ресурсов в сетях Петри [Электронный ресурс].

12. Барендрегт Х. Ламбда-исчисление. Его синтаксис и семантика. — М.: Мир, 1985.

13. Singh D., Ibrahim A. M., Yohanna T., Singh J. N. An overview of the applications of multisets // Novi Sad J. of Mathematics. — 2007. — V. 37, № 2. — P. 73–92.

14. Малинецкий Г. Г. Вычисления на ДНК. Эксперименты. Модели. Алгоритмы. Инструментальные средства [Электронный ресурс].

15. Albert J. Algebraic properties of bag data types // XVII Int. Conf. on Very Large DB. — Spain, 1991. — P. 211–219.

16. Скорняков Л. А. Элементы алгебры. — Москва: Наука, 1986.

О СЛОЖНОСТИ ОДНОЙ ЗАДАЧИ ЦЛП

С. И. Веселов (Нижний Новгород)

Матрица $A \in \mathbf{Z}^{m\times n}$ называется бимодулярной, если $rank\ A = n$ и модули ее $(n \times n)$-миноров не превышают 2. Для произвольного полиэдра P обозначим множество вершин символом $V(P)$, множество целых точек — символом P_Z. В работе [1] доказано несколько утверждений относительно полиэдров $M(A,b) = \{x \in \mathbf{R}^n :\ Ax \le b\}$ и $M_Z(A,b)$.

Теорема 1 [1]. *Если A бимодулярна, $b \in \mathbf{Z}^n$ и $M(A,b)$ имеет размерность n, то $M_Z(A,b)$ непуст.*

Для каждой вершины u полиэдра $M(A,b)$ определим $I(u) = \{i : \sum_{j=1}^n a_{ij}u_j = b_i\}$, $N(u) = \{x : \sum_{j=1}^n a_{ij}x_j \le b_i,\ i \in I(u)\}, \overline{N}(u) = \{x : b_i - 1 \sum_{j=1}^n a_{ij}x_j \le b_i,\ i \in I(u)\}$.

Теорема 2 [1]. $V(M_Z) = \bigcup\limits_{u\in V(M)} V(N_Z(u))$.

Теорема 3 [1]. $V(N_Z(u)) \subseteq \overline{N}(u)$.

Последние теоремы позволяют свести задачу нахождения $\max\{c^Tx :\ x \in M_Z(A,b)\}$ к поиску $\max\{c^Tx :\ x \in \overline{N}_Z(u)\}$.

По поводу следующих терминов можно обратиться к [2, 3].

Неравенство $c^Tx \le c_0$ с целыми коэффициентами называется *отсечением Гомори* для полиэдра P, если $c_0 < max\{c^Tx :\ x \in P\} < c_0 + 1$. Пусть $GH(P)$ множество всех отсечений Гомори для полиэдра P.

Элементарное замыкание $P' \subseteq P$ состоит из точек, удовлетворяющих каждому неравенству из $GH(P)$.

Вычисление P' называется *итерацией Гомори—Хватала.*

Рангом Хватала полиэдра P называется наименьшее целое k, такое, что $P^{(k)} = P_Z$.

Теорема 4 [2]. *Ранг Хватала полиэдра, содержащегося в n-мерном 0-1-кубе, не превышает $n^2(1 + \log\ n)$.*

Из перечисленных выше утверждений выводится следующий результат.

Теорема 5. *Для нахождения $\max\{c^Tx :\ x \in M_Z(A,b)\}$ требуется не более $n^2(1 + \log\ n)$ итераций Гомори—Хватала.*

Работа выполнена при финансовой поддержке РФФИ (проект 09-01-00545-а).

Список литературы

1. Veselov S. I., Chirkov A. J. Integer program with bimodular matrix // Discrete Optimization. — 2009. — V. 6 (2). — P. 220–222.

2. Eisenbrand F., Schulz A. S. Bounds on the chvatal rank of polytopes in the 0/1-cube // Combinatorica. — 2003. — V. 23 (2). — P. 245–261.

3. Схрейвер А. Теория линейного и целочисленного программирования. Т. 2. — М.: Мир, 1991.

4. Шевченко В. Н. Качественные вопросы целочисленного программирования. —М.: Физматлит, 1995.

РЕШЁТКИ ЗАМКНУТЫХ МНОЖЕСТВ СИСТЕМ НЕЗАВИСИМОСТИ

М. Ю. Выплов, В. П. Ильев (Омск)

Предложена характеризация систем независимости в терминах замыкания и показано, что любая конечная решётка изоморфна решётке замкнутых множеств некоторой системы независимости.

Пусть V — непустое конечное множество. Пара $H = (V, \mathcal{A})$, где $\mathcal{A} \subseteq 2^V$ — непустое семейство подмножеств V, называется *системой независимости* на V, если для всех $A, A' \subseteq V$ выполняется *аксиома наследственности*:

(A1) $A \in \mathcal{A}, A' \subseteq A \Rightarrow A' \in \mathcal{A}$.

Множество называется *независимым*, если оно принадлежит $\mathcal{A}$.

Система независимости $M = (V, \mathcal{A})$ называется *матроидом* на V, если выполняется *аксиома пополнения*:

(A2) $A, A' \in \mathcal{A}, |A'| = |A| + 1 \Rightarrow \exists a \in A' \setminus A$: $A \cup \{a\} \in \mathcal{A}$.

Матроид называется *простым*, если $\{u, v\} \in \mathcal{A}$ для всех $u, v \in V$.

Хорошо известно эквивалентное определение матроида в терминах замыкания. Пусть V — непустое конечное множество. Отображение $X \stackrel{\varphi}{\to} \overline{X}$ множества 2^V в себя называется *оператором замыкания*, если для всех X, $Y \subseteq V$ выполняются следующие условия:

(φ1) $X \subseteq \overline{X}$; (φ2) $X \subseteq Y \Rightarrow \overline{X} \subseteq \overline{Y}$; ($\varphi$3) $\overline{\overline{X}} = \overline{X}$.

Множество $X \subseteq V$ называется *замкнутым*, если $X = \overline{X}$.

Непустое конечное множество V вместе с оператором замыкания $X \stackrel{\varphi}{\to} \overline{X}$ называется *комбинаторной геометрией* [1], если для всех $u, v \in V$ и $X \subseteq V$ выполняется *аксиома замены:*

($\varphi 4$) $v \notin \overline{X},\ v \in \overline{X \cup \{u\}} \Rightarrow u \in \overline{X \cup \{v\}}$,

и, кроме того,

($\varphi 5$) $\overline{\emptyset} = \emptyset$ и $\overline{\{v\}} = \{v\}$ для всех $v \in V$.

Опуская условие ($\varphi 5$), получаем определение *комбинаторной предгеометрии* на множестве V.

В следующей теореме, доказательство которой можно найти в [2], установлено взаимно однозначное соответствие между комбинаторными предгеометриями и матроидами.

Теорема 1. 1) *Пусть $M = (V, \mathcal{A})$ — матроид, где V — непустое конечное множество, $\mathcal{A}$ — семейство его независимых подмножеств. Тогда отображение $X \stackrel{\varphi}{\to} \overline{X}$ множества 2^V в себя, определенное по правилу:*

$$\overline{X} = X \cup \{v \in V \ : \ \exists\ A \subseteq X \text{ такое, что } A \in \mathcal{A},\ A \cup \{v\} \notin \mathcal{A}\}, \quad (1)$$

обладает свойствами ($\varphi 1$) – ($\varphi 4$), *причем*

$$\mathcal{A} = \{A \subseteq V \ : \ a \notin \overline{A \setminus \{a\}} \text{ для всех } a \in A\}. \quad (2)$$

2) *И наоборот, если $M = (V, \varphi)$ — комбинаторная предгеометрия, где $\varphi : 2^V \to 2^V$ — оператор замыкания, то семейство $\mathcal{A} \subseteq 2^V$, определенное по правилу* (2), *является семейством независимых множеств матроида, причем имеет место равенство* (1).

Теперь попытаемся дать аналогичное определение системы независимости в терминах замыкания.

Пусть V — непустое конечное множество. Отображение $X \stackrel{\varphi}{\to} \overline{X}$ множества 2^V в себя будем называть *оператором слабого замыкания*, если оно удовлетворяет условиям ($\varphi 1$), ($\varphi 2$).

Аксиому идемпотентности ($\varphi 3$), мы должны заменить более слабым требованием. Рассмотрим следующее условие:

($\varphi 3'$) $\forall X \subset V\ \forall u \in \overline{X} \setminus X\ \forall v \in \overline{X \cup \{u\}} \setminus (X \cup \{u\})$
$\exists w \in X \cup \{u\} : v \in \overline{X \cup \{u\} \setminus \{w\}}$.

Заметим, что при этом $v \in \overline{\overline{X}} \setminus \overline{X}$.

В следующей теореме установлено соответствие между операторами слабого замыкания и системами независимости.

Теорема 2. 1) *Пусть $H = (V, \mathcal{A})$ — система независимости, где V — непустое конечное множество, $\mathcal{A}$ — семейство его независимых подмножеств. Тогда отображение $X \stackrel{\varphi}{\to} \overline{X}$ множества*

2^V *в себя, определенное по правилу* (1), *обладает свойствами* (φ1), (φ2), ($\varphi 3'$) *и* (φ4), *причем имеет место равенство* (2).

2) *И наоборот, если* $\varphi : 2^V \to 2^V$ — *оператор слабого замыкания, удовлетворяющий аксиомам* ($\varphi 3'$) *и* (φ4), *то семейство* $\mathcal{A} \subseteq 2^V$, *определенное по правилу* (2), *удовлетворяет аксиоме наследственности, причем имеет место равенство* (1).

Установленное в теореме 2 соответствие между операторами слабого замыкания, удовлетворяющими аксиомам ($\varphi 3'$) и (φ4), и системами независимости является взаимно однозначным. Поэтому понятие оператора слабого замыкания, удовлетворяющего аксиомам ($\varphi 3'$) и (φ4), можно рассматривать как эквивалентное определение системы независимости. Если $\varphi : 2^V \to 2^V$ — такой оператор, то пару $H = (V, \varphi)$ будем называть *системой независимости.*

Решётка называется *точечной*, если каждый её элемент является точной верхней гранью точек. Решётка называется *полумодулярной*, если для любых её элементов x, y выполняется соотношение $x \wedge y \lessdot x \Rightarrow y \lessdot x \vee y$. Конечная решётка называется *геометрической*, если она является точечной и полумодулярной.

Замкнутые множества матроида образуют решётку, в которой $X \wedge Y = X \cap Y$ и $X \vee Y = \overline{X \cup Y}$.

Системе независимости $H = (V, \varphi)$ сопоставим решетку $L(V)$ замкнутых подмножеств V, упорядоченных по включению. Если $X, Y \in L(V)$, то $X \wedge Y = X \cap Y$, а $X \vee Y$ — минимальное по включению замкнутое множество, содержащее $X \cup Y$.

Следующая теорема раскрывает связь между матроидами и геометрическими решётками.

Теорема 3 (Биркгоф—Уитни) *Решётка* $L(V)$ *замкнутых множеств матроида — геометрическая. Обратно, если* L — *конечная геометрическая решётка с непустым множеством точек* V, *то пара* (V, φ), *где* $\varphi(X) = \{v \in V : v \leq \sup X\}$, *является простым матроидом, а* $f : L \to L(V), f(x) = \{v \in V : v \leq x\}$ — *изоморфизм решёток.*

Нас будет интересовать вопрос: можно ли обобщить теорему Биркгофа—Уитни на системы независимости? Как показано далее, класс решёток замкнутых множеств систем независимости совпадает с классом всех непустых конечных решёток.

Теорема 4. *Для любой непустой конечной решётки* L *существует такая система независимости* $H = (V, \varphi)$, *что решётка* $L(V)$ *всех замкнутых множеств системы* H *изоморфна* L. *Более того, в случае* $|L| > 1$ *можно построить* H *таким образом, что* $\overline{\emptyset} = \emptyset$.

Список литературы

1. Crapo H. H., Rota G.-C. On the foundations of combinatorial theory II: combinatorial geometries. — Cambridge Mass.: MIT Press, 1970.
2. Айгнер М. Комбинаторная теория. — М.: Мир, 1982.

ЗАДАЧА О ТОЖДЕСТВАХ В СИММЕТРИЧЕСКОЙ ГРУППЕ И ЕЕ ПРИЛОЖЕНИЯ

М. Н. Вялый, Р. А. Гимадеев (Москва)

Слово в алфавите $X_s^{\pm 1} = \{x_0, \ldots, x_{s-1}, x_0^{-1}, \ldots, x_{s-1}^{-1}\}$ называется *тождеством в группе* G, если при любой подстановке элементов G вместо переменных x_i получается единичный элемент группы G.

Задача о тождествах в симметрической группе состоит в нахождении минимальной длины $L_s(n)$ непустого несократимого тождества в алфавите из s символов в симметрической группе S_n. (Слово сократимо, если оно содержит подслова вида xx^{-1}, $x^{-1}x$.)

Для однобуквенного алфавита задача тривиальна:

$$L_1(n) = \text{НОК}(1, 2, \ldots, n) = e^{n+o(n)}.$$

Оценки $L_s(n)$ при различных $s > 1$ связаны следующими неравенствами.

Лемма. *Для любых* $s > k > 1$ *выполнено*

$$L_2(n)(3 + 2\log_2 s) \leq L_s(n) \leq L_k(n) \leq L_2(n).$$

Поэтому наиболее интересен случай тождеств в двухбуквенном алфавите. Для этого случая нами получена субэкспоненциальная верхняя оценка.

Теорема 1. $L_2(n) \leq e^{4\sqrt{n}\ln n}$ *при достаточно больших* n.

Получение нижних оценок для $L_2(n)$ — более трудная задача. В частности, из таких оценок следовали бы *верхние* оценки в известной трудной задаче различения слов автоматами.

Задача различения слов автоматами состоит в нахождении минимального числа $A(\ell)$ такого, что для любой пары двоичных слов

u, v длины ℓ найдется детерминированный автомат с не более чем $A(\ell)$ состояниями, который различает эти слова (принимает одно и не принимает другое). Наилучшая известная верхняя оценка $A(\ell) = O(\ell^{2/5}\log^{3/5}\ell)$ принадлежит Робсону [2] и получена еще в 1989 году. Для частного случая обратимых автоматов Робсон получил оценку $O(\sqrt{\ell})$ состояний [3].

Задача различения слов обратимыми конечными автоматами связана с задачей о тождествах в симметрической группе следующим образом. Назовем *перестановочной сложностью* $\nu(w)$ слова $w \in (X_s^{\pm 1})^*$ минимальное n такое, что w не является тождеством в S_n. Ясно, что

$$L_s(n) = \min(|w| : w \in (X_s^{\pm 1})^*,\ n < \nu(w) < +\infty).$$

С другой стороны, для слов специального вида $w = uv^{-1}$, где u, v содержат только положительные вхождения переменных x_i, перестановочная сложность равна минимальному количеству состояний обратимого автомата, различающего слова u, v. Поэтому из второй оценки Робсона имеем оценку перестановочной сложности $\nu(uv^{-1}) = O(\sqrt{\ell})$, $\ell = |uv^{-1}|$.

Мы обобщили метод Робсона и получили степенны́е оценки перестановочной сложности для более широкого класса слов. А именно, слово называется абелево несбалансированным, если порождаемый им маршрут на целочисленной решетке проходит по некоторому ребру неодинаковое количество раз в прямом и обратном направлении.

Теорема 2. *Для абелево несбалансированных слов*

$$\nu(w) = O(\ell^{2/3}\log\ell).$$

Специальные слова вида uv^{-1} являются абелево несбалансированными. Для таких слов оценка теоремы 2 может быть улучшена до $O(\sqrt{\ell})$.

Задачу о тождествах можно интерпретировать как задачу о поиске универсального циклического маршрута для графов размера n аналогично тому, как определяется универсальная обходящая последовательность [1]. С любым набором π_i перестановок степени n можно связать ориентированный граф на n вершинах, ребра которого помечены перестановками из набора: ребро $(v, \pi_i(v))$ получает метку i. (Допускаются петли и параллельные ребра.) Будем называть такие графы регулярными графами с циклической разметкой, сокращенно РЦ-графами.

Слово в алфавите $X_s^{\pm 1}$ порождает маршрут по РЦ-графу — символ x_i означает переход по ребру i в прямом направлении, а символ x_i^{-1} — в обратном. Тождество w в группе S_n порождает циклический маршрут на любом графе на n вершинах. Верно и обратное — любой *универсальный циклический маршрут*, т. е. слово, порождающее циклический маршрут на любом РЦ-графе на n вершинах, является тождеством в S_n. Поэтому из теоремы 1 получаем

Следствие. *Для РЦ-графов на n вершинах существует универсальный циклический маршрут длины $2^{O(\sqrt{n}\log n)}$.*

Более сильным является понятие *универсального реберно сбалансированного маршрута*. Это такое слово, которое порождает на любом графе на n вершинах маршрут, проходящий по каждому ребру одинаковое количество раз в прямом и обратном направлении.

Лемма. *Если для РЦ-графов на n вершинах существует универсальный циклический маршрут длины L, то для РЦ-графов на $\Omega(n/\log n)$ вершинах существует универсальный реберно сбалансированный маршрут длины L.*

Следствие. *Для РЦ-графов на n вершинах существует универсальный реберно сбалансированный маршрут длины $2^{O(\sqrt{n}\log^{3/2} n)}$.*

Задача о тождествах в S_n имеет также отношение к задаче построения графов большого обхвата (обхват — длина наименьшего цикла в графе). Графы, для которых длина кратчайшего тождества в S_n является обхватом, получаются как произведения РЦ-графов с n вершинами. Функция $L_s(n)$ характеризует наибольший обхват таких произведений.

Работа выполнена при финансовой поддержке РФФИ, проекты 08–01–00414 и 09–01–00709, а также гранта поддержки ведущих научных школ НШ-5294.2008.1.

Список литературы

1. Кулямин В. В. Комбинаторика слов и построение тестовых последовательностей // Труды ИСП РАН. — 2004. — Т. 8, вып. 1. — С. 25–40.

2. Robson J. M. Separating strings with small automata // Information Processing Letters. — 1989. — V. 30. — P. 209–214.

3. Robson J. M. Separating words with machines and groups // Informatique théorique et Applications. — 1996. — V. 30. — P. 81–86.

ОЦЕНКИ ЧИСЛА БУЛЕВЫХ ФУНКЦИЙ, ИМЕЮЩИХ АФФИННЫЕ ПРИБЛИЖЕНИЯ ЗАДАННОЙ ТОЧНОСТИ

А. М. Зубков, А. А. Серов (Москва)

Пусть $V_n = (\mathrm{GF}(2))^n$. Обозначим через $\mathbb{F}_2^{V_n}$ и $\mathbb{A}_n$ множества всех булевых и всех аффинных функций от n булевых переменных соответственно, и через $\mathbb{F}_2^{V_n}(r) \subseteq \mathbb{F}_2^{V_n}$ — множество булевых функций, расстояние Хэмминга от которых до множества $\mathbb{A}_n$ не превосходит r. Известно [1], что $\mathbb{F}_2^{V_n}(r) = \mathbb{F}_2^{V_n}$, если $r \geq 2^{n-1} - 2^{n/2-1}$. Определим $x_n(r)$ соотношением

$$r = 2^{n-1} - \sqrt{2^{n-1}\left(n\ln 2 - \tfrac{1}{2}\ln(4\pi n \ln 2) + x_n(r)\right)}.$$

Если $\mathbb{F}_2^{V_n,0}(r)$ — множество всех булевых функций, расстояние Хемминга от которых до множества линейных функций (аффинных с нулевым свободным членом) не превосходит r, то согласно теореме из [2] при $n, r \to \infty$, $x_n(r) \to x \in \mathbb{R}$

$$|\,\mathbb{F}_2^{V_n,0}(r)| = 2^{2^n}\left(B(x) + o(1)\right), \quad \text{где } B(x) = 1 - e^{-e^{-x}}, \tag{1}$$

т. е. при $n \to \infty$ для основной массы булевых функций от n переменных расстояние до множества линейных функций отличается от $2^{n-1} - \sqrt{2^{n-1}\left(n\ln 2 - \frac{1}{2}\ln n\right)}$ на величину порядка $O\left(\sqrt{2^n/n}\right)$.

Нами получены двусторонние оценки для $|\,\mathbb{F}_2^{V_n}(r)|$, которые справедливы при всех неотрицательных $r < 2^{n-1} - 2^{n/2-1}$. Аналогичные оценки получены и для $|\,\mathbb{F}_2^{V_n,0}(r)|$; они показывают, что при $n, r \to \infty$ выражение $2^{2^n} B(x_n(r))$ может не быть правильной асимптотикой для $|\,\mathbb{F}_2^{V_n,0}(r)|$, если $x_n(r) \to \infty$.

Считая равными 0 суммы, в которых верхний предел суммирования меньше нижнего, введем обозначения

$$N_1(n,r) = \sum_{m=0}^{r} C_{2^n}^m, \quad N_2(n,r) = \sum_{m_0=0}^{r-2^{n-2}} C_{2^{n-1}}^{m_0} \sum_{m_1=2^{n-1}-(r-m_0)}^{r-m_0} C_{2^{n-1}}^{m_1},$$

$$N_3(n,r) = \sum_{v=0}^{r-2^{n-2}} \sum_{u=2^{n-1}-r+2v}^{r} C_{2^{n-2}}^{v}\, C_{2^{n-2}}^{u-v}\, S(r-u, r+u-2v-2^{n-1}),$$

$$S(a,b) = \sum_{\substack{g,h\geqslant 0:\\ g+h\leqslant a,\ |g-h|\leqslant b}} C^g_{2^{n-2}}\, C^h_{2^{n-2}}.$$

Теорема 1. a) *Если* $0 \leqslant r < 2^{n-1}$, *то* $|\,\mathbb{F}_2^{V_n}(r)| \leqslant 2^{n+1}N_1(n,r)$ *и*

$$2^{n+1}N_1(n,r) - 4\,C^2_{2^n}N_2(n,r) \leqslant |\,\mathbb{F}_2^{V_n}(r)| \leqslant$$

$$\leqslant 2^{n+1}N_1(n,r) - 4\,C^2_{2^n}N_2(n,r) + 8\,C^3_{2^n}N_3(n,r). \qquad (2)$$

b) *Если* $0 < r < 2^{n-2}$, *то* $|\,\mathbb{F}_2^{V_n}(r)| = 2^{n+1}N_1(n,r)$.

c) *Если* $2^{n-2} \leqslant r < 2^{n-2} + 2^{n-4}$, *то* $|\,\mathbb{F}_2^{V_n}(r)|$ *равно правой части* (2).

Аналог неравенств (2) для $|\,\mathbb{F}_2^{V_n,0}(r)|$ имеет следующий вид:

$$2^nN_1(n,r) - C^2_{2^n}N_2(n,r) \leqslant |\,\mathbb{F}_2^{V_n,0}(r)| \leqslant$$

$$\leqslant 2^nN_1(n,r) - C^2_{2^n}N_2(n,r) + C^3_{2^n}N_3(n,r); \qquad (2')$$

аналоги остальных утверждений теоремы 1 тоже верны (с естественными изменениями).

Используя результаты статьи [3], можно показать, что при $r < 2^{n-1}$

$$\left(\frac{2^n}{r}\right)^r \left(\frac{2^n}{2^n-r}\right)^{2^n-r} \frac{1}{\sqrt{2^{n+1}\pi V\left(1-\frac{r}{2^{n-1}}\right)}} \left(1 - \frac{1}{2^nV\left(1-\frac{r}{2^{n-1}}\right)}\right) <$$

$$< N_1(n,r) < \left(\frac{2^n}{r+1}\right)^{r+1} \left(\frac{2^n}{2^n-r-1}\right)^{2^n-r-1} \frac{1}{\sqrt{2^{n+1}\pi V\left(1-\frac{r+1}{2^{n-1}}\right)}},$$

где $V(z) = (1-z)\ln(1-z) + (1+z)\ln(1+z)$.

Из теоремы 1 следуют неравенства

$$2^{n+1}N_1(n,r)(1-Q(n,r)) \leqslant |\,\mathbb{F}_2^{V_n}(r)| \leqslant 2^{n+1}N_1(n,r),$$

где

$$Q(n,r) = \frac{4\,C^2_{2^n}N_2(n,r)}{2^{n+1}N_1(n,r)} < \frac{2^nN_2(n,r)}{N_1(n,r)}.$$

Теорема 2. *Если* $n \geqslant 10$, $r > 2^{n-2}$ *и* $y = 2^{n-1} - r > 0$, *то*

$$Q(n,r) < \frac{2}{5} \cdot 2^{n/2} \left(\frac{2^{n-2}}{y} + 1 \right)^2 \exp\left\{ -\frac{y^2}{2^{n-1}} \left(1 - \frac{3y}{2^n} \right) \right\}.$$

Следствие. *Если* $n \geqslant 2$, $c > 1$, *то*

$$Q\left(n, 2^{n-1} - \sqrt{cn2^{n-1}} \right) < \frac{1}{2} 2^{3n/2} \exp\left\{ -cn \left(1 - \frac{3\sqrt{cn}}{2^{(n+1)/2}} \right) \right\}.$$

Последнее неравенство показывает, что при любом $c > \frac{3}{2} \ln 2$

$$Q\left(n, 2^{n-1} - \sqrt{cn2^{n-1}} \right) \to 0,\ n \to \infty,$$

т. е. что левые и правые части неравенств (2) и (2') асимптотически эквивалентны, когда $n \to \infty$, $\frac{2^{n-1}-r}{\sqrt{n2^{n-1}}} > \sqrt{\frac{3}{2} \ln 2}$. Согласно [2] эта область близка к области, содержащей основную массу булевых функций, при $n \to \infty$.

Из полученных результатов и [2] следует также, что при $n, r_n \to \infty$ и $x_n(r_n) \to \infty$

$$\frac{|\,\mathbb{F}_2^{V_n,\,0}(r_n)|}{2^{2^n}\,(B(x_n(r_n)) + o(1))} < \frac{2^n N_1(n,r)}{2^{2^n}\,(B(x_n(r_n)) + o(1))} < \frac{e\sqrt{2^{n-1} n \ln 2}}{2^{n-1} - r - 1},$$

т. е. при $2^{n-1} - r - 1 > 3\sqrt{2^{n-1} n \ln 2}$ соотношение (1) дает завышенные оценки числа булевых функций, находящихся на расстоянии не более r от множества линейных функций.

Работа выполнена при поддержке РФФИ, грант 08-01-00078.

Список литературы

1. Логачев О. А., Сальников А. А., Ященко В. В. Булевы функции в теории кодирования и криптологии. — М.: МЦНМО, 2004.

2. Ryasanov B. V. Probabilistic methods in the theory of approximation of discrete functions // Probabilistic Methods in Discr. Math.: Proceedings of the Third International Petrozavodsk Conference. — Moscow: TVP/VSP, 1993. — P. 403–412.

3. Alfers D., Dinges H. A normal approximation for Beta and Gamma tail probabilities // Z. Wahrscheinlichkeitstheor. verw. Gebiete. — 1984. — V. 65. — P. 399–420.

ТЕОРИЯ ДЕТЕРМИНАНТНЫХ ЛАДЕЙНЫХ ПОЛИНОМОВ И ДЕТЕРМИНАНТОВ ПРЯМОУГОЛЬНЫХ МАТРИЦ С ПРИЛОЖЕНИЯМИ К ПЕРЕЧИСЛИТЕЛЬНОЙ КОМБИНАТОРИКЕ

А. М. Каменецкий (Москва)

Пусть A — $m \times n$-матрица над коммутативным кольцом с единицей и $t = \min(m,n)$, $s(\bar{\alpha}) = i_1 + \ldots + i_k$, если $\bar{\alpha} = (i_1, \ldots, i_k)$. По определению,

$$R^{(\det)}(x; A) = 1 + \sum_{1 \le k \le t} x^k \sum_{\bar{\alpha} \in Q_{k,m}} \sum_{\bar{\beta} \in Q_{k,n}} (-1)^{s(\bar{\alpha})+s(\bar{\beta})} \det(A[\bar{\alpha}|\bar{\beta}]),$$

$r_k^{(\det)}(A) = [x^k]R^{(\det)}(x; A)$, $\det(A) = r_t^{(\det)}(A)$.

Теорема 1. *Если $J_{m,n}$ — $m \times n$-матрица, все элементы которой равны 1, $t = \min(m,n)$, то*

$$r_{t-2k-1}^{(\det)}(yJ_{m,n} + A) = r_{t-2k-1}^{(\det)}(A), \quad 0 \le k \le \left[\frac{t-1}{2}\right],$$

$$r_{t-2k}^{(\det)}(yJ_{m,n}+A) = \frac{1+(-1)^{m-n}}{2} r_{t-2k-1}^{(\det)}(A)y + r_{t-2k}^{(\det)}(A), \quad 0 \le k \le \left[\frac{t}{2}\right].$$

Теорема 2. *Пусть A — квадратная матрица порядка n и $\varphi, \psi \in Sym(n)$. Пусть $P(\varphi) = (b_{i,j})_{1 \le i,j \le n}$, $b_{i,j} = 1$, если $j = \varphi(i)$, и $b_{i,j} = 0$, если $j \ne \varphi(i)$. Если $n-1 \le k \le n$, то*

$$r_k^{(\det)}(P(\varphi)AP(\psi^{-1})) = (-1)^{sgn\varphi + sgn\psi} r_k^{(\det)}(A),$$

$$r_n^{(\det)}(A) = (-1)^n r_n(z = -1; A),$$

$$r_{n-1}^{(\det)}(A) = (-1)^{n-1} r_{n-1}(z = -1; A) = \sum_{i,j=1}^{n} (-1)^{i+j} \det(A(i|j)).$$

Теорема 3. *Пусть $A = (a_{i,j})_{1 \le i,j \le n}$ и для $s_j = \sum_{i=1}^n a_{i,j}$ $s_j = s_k$ при всех $j, k, 1 \le j, k \le n$. Тогда*

$$s_1 r_{n-1}^{(\det)}(A) = n \det(A), \quad s_1 \det(yJ_n + A) = (ny + s_1) \det(A).$$

Лемма 1. *Пусть* $k \geq 1, n \geq k+1, p \geq 0, q \geq 0$ *и* $t = \left[\frac{n-1}{k}\right]$. *Тогда существует такая* $\varphi \in Sym(n)$, *что*

$$P(\varphi)\left(\sum_{i=-p}^{q} a_i T_n^{(ki)}\right) P(\varphi^{-1}) = \bigoplus_{l=1}^{k} A_l,$$

$$A_l = \sum_{i=-p}^{q} a_i T_{t+1}^{(i)}, 1 \leq l \leq n - tk; \quad A_l = \sum_{i=-p}^{q} a_i T_t^{(i)}, n - tk + 1 \leq l \leq k.$$

Если $1 \leq n \leq k$, *то* $\sum_{i=-p}^{q} a_i T_n^{(ki)} = a_0 I_n$.

Теорема 4. *Пусть* $k \geq 1, l \geq 0$ *и* $a_1, \ldots, a_k, b_1, \ldots, b_l$ — *свободные образующие свободной группы. Пусть* $f(n)$ — *число линейно несократимых слов,* $g(n)$ — *число циклически несократимых слов длины* n *в алфавите* $a_1, \ldots, a_k, b_1, \ldots, b_l, a_1^{-1}, \ldots, a_k^{-1}$. *Тогда*

$$\sum_{n \geq 1} f(n) x^n = \frac{(2k+l)x + lx^2}{1 - (2k-1+l)x - lx^2},$$

$$g(n) = k + (-1)^n (k-1) + \sum_{s=0}^{[n/2]} \frac{n}{n-s} \binom{n-s}{s} (2k-1+l)^{n-2s} l^s,$$

$$\sum_{n \geq 1} g(n) x^n = \frac{kx}{1-x} - \frac{(k-1)x}{1+x} + \frac{(2k-1+l)x + 2lx^2}{1 - (2k-1+l)x - lx^2}.$$

Доказательство. Следует из теорем 1, 2 и леммы 1; трансферматрица $A = J_{2k+l} - T_{2k+l}^{(-(k+l))} - T_{2k+l}^{(k+l)}$.

Автором также получено элементарное доказательство теоремы 4. Случай $l = 0$ — особо простой, так как $T_{2k}^{(-k)} + T_{2k}^{(k)} = P_{2k}^k$, и формула для $\det(yJ_n + A)$, когда A — групповая матрица, содержится в [1].

На множестве $\mathcal{Q}_t = \cup_{k=0}^{t} Q_{k,t}$ определим квадратную матрицу (обозначим ее $K_t^{(\det)}(a_0, \ldots, a_t) = (a_{\bar{\alpha},\bar{\beta}})_{\bar{\alpha},\bar{\beta} \in \mathcal{Q}_t}$) порядка 2^t следующим образом. $K_0^{(\det)}(a_0) = 1 + a_0$. Пусть $t \geq 1$, $\bar{\alpha} = (i_1, \ldots, i_k) \in Q_{k,t}$. В случае $k = 0$, т. е. $\bar{\alpha} = \varnothing$, имеем: $a_{\bar{\alpha},\bar{\beta}} = a_0$, если $\bar{\beta} = \varnothing$; 1, если

$\bar\beta = (1)$; 0 для остальных случаев. Если же $k \geq 1$ и $i_k < t$, то

$$a_{\bar\alpha,\bar\beta} = \begin{cases} a_0, & \bar\beta = \bar\alpha + 1 = (i_1+1, \ldots, i_k+1); \\ (-1)^s a_{i_s}, & \bar\beta = (1, i_1+1, \ldots, \widehat{i_s+1}, \ldots, i_k+1),\ s \leq k; \\ 1, & \bar\beta = (1, i_1+1, \ldots, i_k+1); \\ 0, & \text{во всех остальных случаях.} \end{cases}$$

Если $k \geq 1$ и $i_k = t$, то

$$a_{\bar\alpha,\bar\beta} = \begin{cases} a_0, & \bar\beta = (i_1+1, \ldots, i_{k-1}+1); \\ (-1)^s a_{i_s}, & \bar\beta = (1, i_1+1, \ldots, \widehat{i_s+1}, \ldots, i_{k-1}+1),\ s \leq k-1; \\ 1+(-1)^k a_t, & \bar\beta = (1, i_1+1, \ldots, i_{k-1}+1); \\ 0, & \text{во всех остальных случаях.} \end{cases}$$

Теорема 5. *Пусть* $n \geq 1$, $t \geq 0$, $0 \leq r \leq \min(n,t)$, $\bar\beta \in Q_{r,\min(n,t)}$, $\bar\alpha \in \mathcal{Q}_t$. *Тогда*

$$R^{(\det)}\left(x; \left(\sum_{i=0}^{t} a_i T_{n+t}^{(i)}\right)\left[N_n | N_n \setminus \bar\beta, n+\bar\alpha\right]\right) =$$

$$= (-1)^{s(\bar\beta)} \sum (-1)^{\mathcal{S}(\bar\beta,\bar\gamma)} (K_t^{(\det)}((-1)^r a_0 x, \ldots, (-1)^r a_t x))^n [L(\bar\alpha)|L(\bar\gamma)],$$

где сумма берется по всем $\bar\gamma \in \cup_{l=r}^{t} Q_{l,t}$, *для которых* $\{\bar\gamma\} \supseteq \{\bar\beta\}$,

$$ind_{\bar\gamma}(j) = l, \ \text{если } \bar\gamma = (i_1, \ldots, i_k), \ j = i_l, \ 1 \leq l \leq k,$$

$\mathcal{S} = \sum_{j \in \{\bar\beta\}} ind_{\bar\gamma}(j)$.

Теорема 6. *Пусть* $t \geq 0, 0 \leq r \leq t$. *Тогда для всех* $n \geq 1$

$$R^{(\det)}\left(x; \sum_{i=0}^{t} a_i T_n^{(-r+i)}\right) =$$

$$= \sum (K_t^{(\det)}((-1)^r a_0 x, \ldots, (-1)^r a_t x))^n [L(N_r)|L(\bar\gamma)],$$

где сумма берется по всем $\bar\gamma \in \cup_{l=r}^{t} Q_{l,t}$, *для которых* $\{\bar\gamma\} \supseteq N_r$.

Отсюда автоматически выводится важная с точки зрения практических вычислений явная формула для производящей функции.

Теорема 7. *Пусть* $t \geq 0$ *и* $a_0, \ldots, a_t$ — *независимые переменные над полем* $\mathcal{K}$. *Тогда полином* $\det(xI_{2^t} - K_t^{(\det)}(a_0, \ldots, a_t))$ *неприводим над полем рациональных функций* $\mathcal{K}(a_0, \ldots, a_t)$.

Список литературы

1. Каменецкий А. М. Перманенты и детерминанты групповых матриц // Сборник трудов семинара по дискретной математике и ее приложениям (1990). — М.: Изд-во мех-мат ф-та МГУ, 1997. — С. 72–73.

РАЗВИТИЕ МЕТОДА ТРАНСФЕР-МАТРИЦЫ В ПЕРЕЧИСЛИТЕЛЬНОЙ КОМБИНАТОРИКЕ. II: ОПЕРАЦИЯ СЛИЯНИЯ КОГЕРЕНТНЫХ СОСТОЯНИЙ

Л. М. Коганов (Москва)

Работа продолжает и развивает серию публикаций [1, 2]. Так, [1] мы будем называть I частью работы (основное название сохранено). Далее сохраняются принятые в I части определения, обозначения и общая терминология.

Определение. *Эквивалентность* или *когерентность* (согласованность) двух состояний — вершин A и B (далее к.с. — когерентные состояния) графа переходов G в стандартном объемлющем двухполюснике [1] характеризуется обязательным одновременным выполнением первых 4-х из 5-ти указанных ниже условий. Мы считаем двухполюсник приведённым: веса параллельных дуг/петель просуммированы.

1. Системы непосредственных предшественников для A и B совпадают. 2. Системы непосредственных последователей для A и B совпадают. 3. Наличие/отсутствие петель в состояниях A и B совпадают (можно отнести к условию 2). 4. Численно или же буквенно совпадают нагрузки соответствующих дуг/петель. 5* (Несвязанность). Эквивалентные состояния не предшествуют непосредственно друг другу, иными словами, не связаны друг с другом равнозагруженными антипараллельными дугами.

Примечание 1. В случае выполнения условия 5* условие 4 можно ослабить, требуя в нём равной загрузки лишь для соответствующих *исходящих* дуг (в т. ч. петель). Отметим, что невыполнение условия 5* приводит к естественному обобщению и модификации правила слияния к.с. (см. ниже). Образование же приведённой системы уравнений совершенно аналогично. При этом дуга между первоначальными к.с. играет роль "внутреннего переключателя" внутри укрупнённого состояния после слияния. Вес одной из антипараллельных

дуг суммируется с весом петли. Если же петли до слияния отсутствуют, то после слияния образуется новая петля за счёт "внутреннего переключателя".

Основное предложение. Порядок (размерность) системы (1) части I может быть понижен на (как минимум — см. далее) единицу введением нового сложного состояния $\{A, B\}$ с потенциалом $Z_A + Z_B = Z_{\{A,B\}}$, фигурирующем в качестве нового неизвестного в приведённой системе (1′) уравнений.

Она образуется из (1) так. Сложение уравнений, в левых частях которых стоят Z_A и, соответственно, Z_B, приводит к одному уравнению, но уже со сложным потенциалом $Z_{\{A,B\}}$ укрупнённого состояния $\{A, B\}$, полученного слиянием к.с. A и B. В остальных уравнениях системы (1) из части I в случае когерентности A и B потенциалы Z_A и Z_B либо одновременно отсутствуют — коэффициенты при них суть нули, либо входят одновременно с одним и тем же коэффициентом, равным, допустим, μ (по условиям 2 и 4 определения). Тогда группируем в этом уравнении указанные члены (слагаемые), представляя их в виде:

$$\mu Z_A + \mu Z_B = \mu(Z_A + Z_B) = \mu \cdot Z_{\{A,B\}}.$$

Таким образом, в случае когерентности состояний A и B путём анализа исходной системы уравнений (1) части I , группировкой потенциалов Z_A и Z_B, выделением в каждом, кроме первых двух вышеуказанных, уравнении их суммы $Z_A + Z_B = Z_{\{A,B\}}$ в виде потенциала укрупнённого состояния $\{A, B\}$ удаётся понизить порядок исходной системы на 1.

Точно такая же группировка — уединение двух слагаемых Z_A и Z_B с одним и тем же общим множителем осуществляется в формуле (2) части I по условиям 2 и 4 настоящего определения, что влечёт в итоге более простое, нежели с помощью (1)–(2) части I нахождение искомой рациональной производящей функции путей, идущих из источника в сток, как передаточной функции двухполюсника с "зашитым" графом переходов G , преобразованным операцией слияния к.с. A и B в новый граф G' *с той же самой передаточной функцией.*

Следствие (правило укрупнения к.с.). *Веса дуг, ведущих в укрупнённое состояние, получаются сложением* (*удвоением*) *весов соответствующих дуг, входящих в к.с. Веса исходящих дуг* (*к ним относятся и петли*) *после слияния остаются без изменений.*

Об антипараллельных равнозагруженных дугах, соединяющих исходные к.с., — см. выше примечание 1 к условию 5*.

Примечание 2. В случае выполнения условия 5* число к.с. в операции одновременного слияния может быть любым, начиная с 2. И даже в случае выполнения условия 5* несвязанности процедура слияния может быть лишь одновременной для всех к.с. сразу и без исключения какого-либо из них, поскольку в случае числа к.с., равного 3 и более, эта процедура не является ассоциативной, ибо слияние первых двух к.с. приводит к вершине, не когерентной с третьей, в силу правила укрупнения для весов входящих дуг и в силу условия 4 определения (см., впрочем, возможность ослабления условия 4 выше в примечании 1).

В качестве одной из простых иллюстраций вышеизложенного можно разобрать пример 4.1.2 из [3] , где в двухполюсник заключается орграф с тремя состояниями: $N(North)$, $E(East)$, $W(West)$, и стандартно [2] перечисляются слова в трёхбуквенном алфавите $\{N, E, W\}$ с запретом подслов (соседства символов) EW и WE в соответствии с длинами слов. При этом состояния E и W суть к.с. (и даже удовлетворяют условию 5* несвязанности из определения). Система уравнений после слияния E и W в $\{E, W\}$ состоит из двух уравнений, соответствующая передаточная функция легко находится (можно сразу положить Z_e равным 1).

Точно также осуществляется приведение систем балансов потенциалов в [4; задача 2.4.6], после формирования графа переходов в задаче М595 из "Задачника Кванта" [5], при выводе формулы для числа циклически несократимых слов предписанной длины в свободной конечнопорождённой группе ранга k [6, 7] и в ряде других примеров.

Автор благодарит В. А. Лисковца (Минск, Институт математики НАН Беларуси) за проверку основного предложения и следствия из него.

Список литературы

1. Коганов Л. М. Развитие метода трансфер-матрицы в перечислительной комбинаторике // Дискретные модели в теории управляющих систем: VIII Международная конференция, Москва, 6–9 апреля 2009 г.: Труды. — М.: Издательский отдел факультета ВМиК МГУ им. М. В. Ломоносова; МАКС Пресс, 2009. — С. 130–131.

2. Коганов Л. М. Передаточная функция в перечислительной комбинаторике // Вестник МГПУ. Сер. Информатика и информатизация образования. — 2008. — № 1 (12). — С. 30–39.

3. Стенли Р. Перечислительная комбинаторика. —М.: Мир, 1990.

4. Гульден Я., Джексон Д. Перечислительная комбинаторика. — М.: Наука. Гл. ред. физ.- мат. лит., 1990.

5. Задачник "Кванта": Математика. Часть 3. — М.: Бюро Квантум, 1997.

6. Коганов Л. М. Число циклически несократимых слов в алфавите свободной группы конечного ранга // Кибернетика и системный анализ. — 2007. — Т. 43, № 4. — С. 39–48.

7. Коганов Л. М. Суммационные уравнения и их применения в перечислительной комбинаторике // Материалы IX Международного семинара "Дискретная математика и её приложения", посвящённого 75-летию со дня рождения академика О. Б. Лупанова (Москва, МГУ, 18–23 июня 2007 г.). — М.: Изд-во механико-математического факультета МГУ, 2007. — С. 215–218.

ОДНА КОМБИНАТОРНАЯ МОДЕЛЬ В ЗАДАЧАХ ТЕОРИИ СЛУЧАЙНЫХ РАЗМЕЩЕНИЙ

Н. А. Колокольникова, А. С. Кузнецов (Иркутск)

Применение специальных комбинаторных моделей, в частности, схем последовательных испытаний, проводимых в переменных условиях, оказывается эффективным при решении разнообразных задач теории случайных размещений. В данной работе при помощи одной такой модели проводится исследование ряда случайных величин, которые появляются в процессе решения задач теории случайных размещений.

Ф-схема последовательных испытаний. Пусть проводятся последовательные испытания по схеме "успех-неуспех". Обозначим ξ_n — число успехов в n испытаниях. Предположим, что условные вероятности успехов имеют следующую структуру:

$$P\{\xi_n = k+1 | \xi_{n-1} = k\} = 1 - P\{\xi_n = k | \xi_{n-1} = k\} = \alpha_{n-1}(c-k), \quad (1)$$

$$k = \overline{0, \min(c, n-1)}, \ n = \overline{1, \infty},$$

где c — некоторое большое натуральное число, $\alpha_{n-1}(n = \overline{1, \infty})$ — вообще говоря, произвольные положительные числа, такие, что $0 \leq \alpha_{n-1}(c-k) \leq 1$ при каждом k. Тогда распределение величины ξ_n запишется [1]:

$$P\{\xi_n = k\} = \Phi_k^n(c)_k \prod_{i=0}^{n-1} \alpha_i, k = \overline{0, \min(n, c)}, \quad (2)$$

где $(c)_0 = 1,\ (c)_k = \prod\limits_{j=0}^{k-1}(c-j),\ k \geq 1;\ \Phi_k^n$ — комбинаторные числа, строящиеся на базах $\{\frac{1}{\alpha_i} - c\}_{i=0}^{\infty}, \{i\}_0^{\infty}$. Числа Φ_k^n могут быть определены следующим образом:

$$\Phi_k^n = \Phi_{k-1}^{n-1} + (\frac{1}{\alpha_{n-1}} - c + k)\Phi_k^{n-1},\quad k = \overline{0,n},\ n = \overline{1,\infty},$$

причем $\Phi_n^n = 1, n = \overline{1,\infty}, \Phi_k^n = 0$, если $k < 0$ или $n < k$.

Распределение вида (2), получаемое при любом конкретном наборе $\{\alpha\}_0^{\infty}$, называется Ф-распределением. Исследование Ф-распределения проводилось в [1].

Задача о размещении случайного числа частиц [2]. Пусть имеется N ячеек, в которые независимо друг от друга, равновероятно размещаются частицы. Число размещаемых частиц ν — случайная величина, распределение которой известно. Рассмотрим величину $\eta = \eta_\nu$ — число непустых ячеек после размещения ν частиц.

Имеется n частиц, причем каждая из них либо размещается в одну из N ячеек, либо вообще не подлежит размещению. Пусть p_{i-1} — вероятность того, что i-я частица будет участвовать в процессе размещения, $q_{i-1} = 1 - p_{i-1},\ i = \overline{1,n}$. Таким образом число размещаемых частиц имеет обобщенное биномиальное распределение.

Используем схему последовательных испытаний типа "успех-неуспех". Успехом будет считаться попадание размещаемой частицы в пустую ячейку. Введем в рассмотрение p_{nk} — вероятность успеха в n-м испытании, если в предыдущих $n-1$ испытаниях был зафиксирован $k-1$ успех. В данной задаче $p_{nk} = p_{n-1}\frac{N-k}{N}$. Очевидно, что структура условной вероятности имеет вид (1), а, следовательно, для решения данной задачи может быть применена Ф-схема последовательных испытаний. Тогда распределение числа непустых ячеек после размещения $\nu = \nu(n)$ частиц будет следующим:

$$P\{\eta = k\} = \frac{(N)_k}{N^n}\Phi_k^n \prod_{i=0}^{n-1} p_i,\ k = \overline{1, \min(n, N)}.$$

Также для случайной величины η при помощи данной комбинаторной модели были получены условия выполнимости закона повторного логарифма:

Теорема. *Пусть* $\eta_n = \eta_\nu - M\eta_\nu$. *Обозначим* $B_n = D\eta_\nu$. *Если* $\exists\ 0 < \delta < 1 : \forall i = \overline{1,n}\ \ \delta < \frac{p_{i-1}}{N^{i-1}} \cdot \prod\limits_{k=0}^{i-2}(N - p_k) < (1-\delta)$, *то при* $n \to \infty$

$\limsup_{n\to\infty} \frac{\eta_n}{\sqrt{2B_n lnlnn}} = 1$ *почти наверное.*

Размещение случайного числа комплектов. Пусть имеется N ячеек, в которые независимо друг от друга размещается r комплектов. Объемы комплектов постоянны и равны m. Каждый комплект будет участвовать в процессе размещения с вероятностью p и с вероятностью $q = 1 - p$ — нет. Рассматривается величина ξ_n — количество непустых ячеек после размещения всех комплектов.

Как и в предыдущей задаче, используется схема испытаний "успех-неуспех", успехом считается попадание частицы в пустую ячейку. Условные вероятности p_{nk} в данном случае имеют вид:

$$p_{nk} = \frac{C_r^{[\frac{n-1}{m}]} \cdot p^{[\frac{n-1}{m}]} \cdot q^{r-[\frac{n-1}{m}]} \cdot (N-m+k)}{N-m+[\frac{n-1}{m}]m+1},$$

где $n = \overline{1,\infty}$, $k = \overline{1,n-1}$. Структура условных вероятностей имеет вид (1), а, следовательно, закон распределения случайной величины будет

$$P\{\xi_n = k\} = \Phi_k^n \cdot \prod_{i=1}^{n} \frac{C_r^{[\frac{i-1}{m}]} \cdot p^{[\frac{i-1}{m}]} \cdot q^{r-[\frac{i-1}{m}]}}{N-m+[\frac{i-1}{m}]m+1} \cdot \prod_{j=0}^{k-1}(N-m+j), \quad (3)$$

где $n = \overline{1,\infty}$, $k = \overline{1,n-1}$. Использование свойств чисел Φ_k^n и Ф-распределения позволило исследовать свойства распределения (3) и получить полный спектр предельных теорем.

Список литературы

1. Колокольникова Н. А. Предельные теоремы для числа успехов в одной схеме зависимых испытаний // Иркут. ун-т. — Иркутск, 1992. — Деп. в ВИНИТИ 26.02.92, № 649.

2. Колокольникова Н. А., Ефремова А. С. Комбинаторные числа и размещение случайного числа частиц // Материалы VIII Международного семинара "Дискретная математика и ее приложения" (2–6 февраля 2004 г.). — М.: Изд-во мех-ма. ф-та МГУ, 2004. — С. 204–208.

3. Докин В. Н., Жуков В. Д., Колокольникова Н. А., Кузьмин О. В., Платонов М. Л. Комбинаторные числа и полиномы в моделях дискретных распределений. — Иркутск: Изд-во Иркут. ун-та, 1990.

ОБ ОЦЕНКАХ СЛОЖНОСТИ РЕШЕНИЯ ЗАДАЧИ О РАНЦЕ НА ПАРАЛЛЕЛЬНЫХ СИСТЕМАХ

Р. М. Колпаков, М. А. Посыпкин (Москва)

Рассмотрим одну из задач дискретной оптимизации — задачу о ранце, в которой целевая функция линейна, а допустимое множество задается линейными ограничениями на булевы переменные:

$$\begin{cases} f(x) = \sum_{i=1}^{n} p_i x_i \to \max; \\ \text{при условиях} \\ \sum_{i=1}^{n} w_i x_i \le C; \\ x_i \in \{0,1\},\ i = 1, \ldots, n. \end{cases}$$

Одним из методов, применяемых для решения этой задачи, является метод ветвей и границ (МВГ). Известно [1], что существуют наборы коэффициентов, для решения которых требуется число шагов МВГ, экспоненциально зависящее от n. В связи с высокой вычислительной сложностью, при решении задачи о ранце методом ветвей и границ нередко применяют методы параллельных и распределенных вычислений [2].

Рассмотрим следующую схему реализации МВГ, подходящую для практически любой параллельной или распределенной платформы. Предположим, что имеется система, состоящая из бесконечного числа одинаковых процессоров. Один из процессоров выполняет некоторое число итераций МВГ, в результате которых полностью обрабатываются первые k ярусов дерева ветвления. Полученные подзадачи передаются для обработки другим процессорам (по одной на процессор). Каждая подзадача полностью решается, после чего производится объединение полученных результатов, из которых выбирается максимум. Первый этап (до передачи подазач) алгоритма выполняется только одним процессором, а на втором этапе процессоры работают параллельно. Приведенный алгоритм назовем *фронтальным*.

Число k ярусов дерева ветвления, обрабатываемых на первом этапе работы фронтального алгоритма, будем называть *глубиной* фронтального алгоритма. *Параллельная вычислительная сложность* фронтального алгоритма естественным образом определяется как сумма числа шагов, сделанных на первом этапе работы алгоритма, и максимального числа шагов, потребовавшихся для решения подзадач, обработанных на втором этапе работы алгоритма.

В данной работе исследуется вопрос о выборе числа k уровней дерева ветвления, которые нужно обработать на первом этапе, обеспечивающих минимальное значение параллельной вычислительной

сложности фронтального алгоритма. Рассматривается пример задачи о ранце, впервые предложенный в работе [3]:

$$\begin{cases} \sum_{i=1}^{n} 2x_i \to \max, \\ \text{при условиях} \\ \sum_{i=1}^{n} 2x_i \le 2l+1, \\ x_i \in \{0,1\}, i = 1, \ldots, n, \end{cases} \tag{1}$$

где $n/3 \le l \le 2n/3$. В [1] доказано, что число последовательных шагов МВГ для решения задачи (1) составляет $2\binom{n+1}{l+1} - 1$.

Обозначим через $P_{n,l}(k)$ параллельную вычислительную сложность фронтального алгоритма глубины k для решения задачи (1), через $P^*_{n,l}$ минимальное значение величины $P_{n,l}(k)$ для заданных значений n и l, и через $k^*(n,l)$ величину параметра k, при которой достигается данное минимальное значение. Нами доказана справедливость следующего утверждения для параллельной вычислительной сложности решения задачи (1) фронтальным алгоритмом.

Утверждение. *При $n \to \infty$ и $n/3 \le l \le 2n/3$ выполняются соотношения*

$$k^*(n,l) = n/2 - \frac{1}{4}\log_2 n + O(1), \qquad P^*_{n,l} \asymp \frac{2^{\frac{n}{2}}}{\sqrt[4]{n}},$$

где запись $f(x) \asymp g(x)$ означает одновременное выполнение соотношений $f(x) = O(g(x))$ и $g(x) = O(f(x))$.

Работа выполнена при финансовой поддержке РФФИ, проект 09-07-00352-а.

Список литературы

1. Колпаков Р. М., Посыпкин М. А. Асимптотическая оценка сложности метода ветвей и границ с ветвлением по дробной переменной для задачи о ранце // Дискретн. анализ и исслед. опер. — 2008. — Т. 15, № 1. — С. 58-81.

2. Посыпкин М. А., Сигал И. Х. Исследование алгоритмов параллельных вычислений в задачах дискретной оптимизации ранцевого типа // ЖВМ и МФ. — 2005. — 45 (10). — 2005, С. 1801–1809.

3. Финкельштейн Ю. Ю. Приближенные методы и прикладные задачи дискретного программирования. — М.: Наука, 1976.

ОБ ОДНОМ ИНВОЛЮТИВНОМ АВТОМОРФИЗМЕ БЕРНСАЙДОВОЙ ГРУППЫ $B_0(2,5)$

А. А. Кузнецов, А. К. Шлёпкин (Красноярск)

Пусть $B_0(2,5)$ — максимальная универсальная конечная двупорожденная группа периода 5 порядок которой равен 5^{34} [1, 2].

Положим $\{1,2\}$ — образующие группы $B_0(2,5)$ и φ_0 — автоморфизм порядка 2 данной группы следующего вида:

$$\varphi_0 : \begin{cases} 1 \to 1^{-1} \\ 2 \to 2^{-1}. \end{cases}$$

Пусть $C_{B_0(2,5)}(\varphi_0)$ — централизатор автоморфизма φ_0 в $B_0(2,5)$. Далее для краткости будем обозначать $C_{B_0(2,5)}(\varphi_0)$ через C.

Основным результатом настоящей работы является следующая

Теорема. *Для C имеют место следующие утверждения:*

1) $|C| = 5^{16}$.

2) $C = X \times \langle x_5 \rangle$, *где* $\langle x_5 \rangle$ — *центр группы* $B_0(2,5)$, $X = \langle x_1, x_2, x_3, x_4 \rangle$ — *группа, со следующими свойствами:*

X имеет нормальную абелеву подгруппу H_2 и $|H_2| = 5^{11}$;

$X/H_2 = \langle x_1 H_2 \rangle \times \langle x_2 H_2 \rangle \times \langle x_3 H_2 \rangle \times \langle x_4 H_2 \rangle$;

$|X| = 5^{15}$.

3) 5 — *минимальное число порождающих C.*

4) *Ступени разрешимости и нильпотентности для C равны* 2 *и* 4, *соответственно.*

Работа выполнена при финансовой поддержке АВЦП "Развитие научного потенциала высшей школы" (проект 2.1.1/3023), а также гранта РФФИ (проект 09-01-00717-а).

Список литературы

1. Кострикин А. И. Решение ослабленной проблемы Бернсайда для показателя 5 // Изв. АН СССР. Сер. мат. — 1955. — Т. 19, № 3. — С. 233–244.

2. Havas G., Wall G., Wamsley J. The two generator restricted Burnside group of exponent five // Bull. Austral. Math. Soc. — 1974. — V. 10. — P. 459–470.

РАЗМЕЩЕНИЕ ЧАСТИЦ В ЯЧЕЙКИ С ОГРАНИЧЕННОЙ ЕМКОСТЬЮ И КОМБИНАТОРНЫЕ ЧИСЛА Λ_n^k

А. С. Кузнецов (Иркутск)

Применение комбинаторных объектов, в частности, комбинаторных чисел, помогает при решении теоретико-вероятностных задач. В данной работе введение комбинаторных объектов дало возможность получить явный вид распределения случайных величин, которые возникают в процессе решения задачи о размещении частиц в ячейки ограниченной емкости.

Постановка задачи. Пусть имеется N ячеек, в которые независимо друг от друга, равновероятно размещаются частицы. Но, в отличие от классической постановки задачи, считается, что емкость ячейки равна 2, т. е. при попадании в ячейку двух частиц, ячейка перестает участвовать в процессе размещения. Ставится задача отыскания явного вида распределения числа пустых ячеек, а также числа ячеек, содержащих ровно одну и числа ячеек, содержащих две частицы.

Число ячеек, содержащих две частицы. Пусть $\mu_2(n)$ — число ячеек, содержащих две частицы после размещения n частиц. Явный вид распределения случайной величины $\mu_2(n)$ был получен при помощи применения схемы последовательных испытаний типа "успех-неуспех". Успехом будем считать попадание очередной размещаемой частицы в ячейку, где уже находится одна частица. Рассмотрим величину ξ_n — число успехов после n испытаний. Очевидно, что $\xi_n = \mu_2(n)$. Нетрудно видеть, что $P\{\xi_n = 0\} = \frac{(N)_n}{N^n}$. Обозначим через $p_{n,k}$ вероятность успеха в n-м испытании, если в предыдущих $n-1$ испытаниях было зафиксированно k успехов, $q_{n,k}$ — вероятность неуспеха при тех же условиях. Структура этих вероятностей будет следующая:

$$p_{n,k} = \frac{n-1-2k}{N-k},\ q_{n,k} = \frac{N-k-(n-1-2k)}{N-k}, k = \overline{0, [n/2]}.$$

Явный вид распределения величины ξ_n, а, следовательно, и величины $\mu_2(n)$ будет выглядит так:

$$P\{\xi_n = k\} = \\ = \Lambda_n^k \frac{N(N-1)\cdot\ldots\cdot(N-n+k+1)}{(N-k)^{n-2k}(N-k+1)^{n-2k+2}(N-k+2)^{n-2k+3}N^{n-k+1}},$$

где числа Λ_n^k определяются следующим образом: при $n \geq 2k$

$$\Lambda_n^k = N \cdot \ldots \cdot (N-k+1)\Lambda_{n-1}^k + (n-2k+1)(N-k)^{n-2k}\Lambda_{n-1}^{k-1}$$

$$\Lambda_2^1 = 1,\ \Lambda_{2k}^k = \Lambda_{2k-1}^{k-1}.$$

Если $n < 2k$, то $\Lambda_n^k = 0$.

Число пустых ячеек и число ячеек, содержащих одну частицу. Пусть $\mu_0(n)$ — число пустых ячеек после размещения n частиц. Вновь используем схему испытаний "успех-неуспех". Успехом будет считаться попадание очередной размещаемой частицы в пустую ячейку. Введем в рассмотрение величину ν_n — число успехов в n испытаниях. Очевидно, что $\mu_0(n) = N - \nu_n$. Обозначим, как и прежде, через $p_{n,k}$ и $q_{n,k}$ соответственно вероятность успеха и неуспеха при условиях, описанных выше. Нетрудно показать, что они будут иметь вид:

$$p_{n,k} = \frac{N-k}{N-n+k+1},\ \ q_{n,k} = \frac{2k+1-n}{N-n+k+1},$$

$$k = \overline{0,N},\ \ n = \overline{k,2k}.$$

Исходя из этого, был получен явный вид распределения величины ν_n, а также величины $\mu_0(n)$:

$$P\{\mu_0(n) = N-k\} = P\{\nu_n = k\} = \\ = \frac{(N)_k}{N^{k+1}(N-1)^k \cdot \ldots \cdot (N-n+k)^{2k-n}} B_n^k,$$

где B_n^k — это комбинаторные числа, определяемые следующим рекуррентным соотношением:

$$B_n^k = N\cdot(N-1)\cdot\ldots\cdot(N-n+k+1)B_{n-1}^{k-1} + (2k-n+1)(N-n+k)^{2k-n}B_{n-1}^k,$$

где $k = \overline{1,N},\ n = \overline{k,2k},\ B_k^k = 1$.

Теперь перейдем к отысканию распределения величины $\mu_1(n)$ — числа ячеек, содержащих одну частицу. Для нее верно следующее равенство: $\mu_1(n) = \nu_n - \xi_n$. Исходя из этого, имеем: $P\{\mu_1(n) = k\} = P\{\nu_n - \xi_n = k\} = \sum\limits_{i=0}^{n-k} P\{\nu_n = k+i\}P\{\xi_n = i | \nu_n = k+i\}$,
где $P\{\xi_n = k_1 | \nu_n = k_2\} = 1$ при $n - k_1 = k_2$ и $P\{\xi_n = k_1 | \nu_n =$

$k_2\} = 1$ в противном случае. Тогда сумма будет иметь всего одно слагаемое, отличное от нуля. Этим слагаемым будет слагаемое с номером $i = \frac{n-k}{2}$, т. е. явный вид распределения величины $\mu_1(n)$ будет следующим:

$$P\{\mu_1(n) = k\} = P\{\nu_n = \frac{n+k}{2}\},$$

где $k \le n \le 2k$.

Таким образом, в процессе решения задачи теоретико-вероятностного характера возникли новые комбинаторные объекты. Изучены некоторые свойства чисел Λ_n^k и B_n^k, получены рекуррентные соотношения для них. Также найдено рекуррентное соотношение для производящей функции чисел Λ_n^k, которое может быть полезно для исследования не только свойств этих чисел, но и вероятностных распределений, связаных с ними.

Пусть $P_k(x)$ — производящая функция чисел Λ_n^k. Полученные рекуррентные соотношения для производящей функции имеют следующий вид:

$$P_k(x) = \frac{x^2 \frac{d}{dx} P_{k-1}((N-k)x) - 2(k+1)xP_{k-1}((N-k)x)}{(1-(N)_k x)(N-k)^{2k-1}}, \quad k > 1,$$

$$P_1(x) = \frac{x^2}{(1-Nx)(1-x(N-1))}.$$

ПЛОСКИЕ СЕЧЕНИЯ ПИРАМИДЫ ПАСКАЛЯ И ПОЛНЫЕ ПОКРЫТИЯ ПРЯМОУГОЛЬНИКОВ

О. В. Кузьмин (Иркутск), М. В. Серёгина (Чита)

Рассматриваются полные покрытия прямоугольника размера $1 \times$ $\times n$ прямоугольниками размера $1 \times q$, $1 \times \frac{q}{q_1}(p_1+q_1)$, $1 \times \frac{q}{q_2}(p_2+q_2)$, $p_1, p_2 \in Z$, $q_1, q_2, n \in N$, $\frac{p_i}{q_i} > -1, i = 1, 2$, не перекрывающими друг друга. Высота покрывающих прямоугольников совпадает с высотой покрываемого прямоугольника. Два покрытия считаются различными, если они отличаются либо порядком расположения, либо составом покрывающих элементов. Если $q = \frac{q}{q_1}(p_1 + q_1)$ и/или

$q = \frac{q}{q_2}(p_2 + q_2)$ и/или $\frac{q}{q_1}(p_1 + q_1) = \frac{q}{q_2}(p_2 + q_2)$, то соответствующие прямоугольники должны быть разных цветов. Такие покрытия назовем *полными*.

Пирамидой Паскаля [1] называем трехгранный пирамидальный массив, элементы которого удовлетворяют следующим рекуррентным соотношениям:

$$\begin{pmatrix} n+1 \\ k,l \end{pmatrix} = \begin{pmatrix} n \\ k-1,l \end{pmatrix} + \begin{pmatrix} n \\ k,l-1 \end{pmatrix} + \begin{pmatrix} n \\ k,l \end{pmatrix}$$

с граничными условиями $\begin{pmatrix} 0 \\ 0,0 \end{pmatrix} = 1$, $\begin{pmatrix} n \\ k,l \end{pmatrix} = 0$, если $\min(n,k,l, n-k-l) < 0$.

Введем в рассмотрение суммы $S_n\left(\frac{p_1}{q_1}, \frac{p_2}{q_2}\right)$, $p_1, p_2 \in Z$, $q_1, q_2, n \in N$, n-х сечений [2–4] пирамиды Паскаля. Обозначим $q = \text{НОК}(q_1, q_2)$.

Теорема. *Число различных полных покрытий равно*

$$S_n\left(\frac{p_1}{q_1}, \frac{p_2}{q_2}\right) = \sum_{m=0}^{\left[\frac{q_2 n}{q(p_2+q_2)}\right]} \sum_{r=0}^{\left[\frac{q_1 n}{q(p_1+q_1)}\right]} \begin{pmatrix} \frac{n}{q} - \frac{p_2}{q_2}m - \frac{p_1}{q_1}r \\ r,m \end{pmatrix}, \quad n \geq 1.$$

Доказательство. Обозначим $x_{m,r}$ — число способов, которыми можно расположить m прямоугольников размера $1 \times \frac{q}{q_2}(p_2+q_2)$ и r прямоугольников размера $1 \times \frac{q}{q_1}(p_1+q_1)$, а также прямоугольники размера $1 \times q$ внутри прямоугольника размера $1 \times n$, не перекрывая друг друга, $n \geq 1$. Если $q = \frac{q}{q_1}(p_1+q_1)$ и/или $q = \frac{q}{q_2}(p_2+q_2)$ и/или $\frac{q}{q_1}(p_1+q_1) = \frac{q}{q_2}(p_2+q_2)$, то соответствующие прямоугольники рассматриваем разных цветов. Тогда число различных полных покрытий равно:

$$\sum_{m=0}^{\left[\frac{q_2 n}{q(p_2+q_2)}\right]} \sum_{r=0}^{\left[\frac{q_1 n}{q(p_1+q_1)}\right]} x_{m,r}.$$

Найдем $x_{m,r}$:

$$x_{m,r} = \frac{P_{\frac{n}{q} - \frac{p_2}{q_2}m - \frac{p_1}{q_1}r}}{P_m \cdot P_r \cdot P_{\frac{n}{q} - \left(\frac{p_2}{q_2}+1\right)m - \left(\frac{p_1}{q_1}+1\right)r}} = \begin{pmatrix} \frac{n}{q} - \frac{p_2}{q_2}m - \frac{p_1}{q_1}r \\ r,m \end{pmatrix}.$$

Таким образом, число различных полных покрытий равно:

$$\sum_{m=0}^{\left[\frac{q_2 n}{q(p_2+q_2)}\right]} \sum_{r=0}^{\left[\frac{q_1 n}{q(p_1+q_1)}\right]} \binom{\frac{n}{q} - \frac{p_2}{q_2}m - \frac{p_1}{q_1}r}{r, m} = S_n\left(\frac{p_1}{q_1}, \frac{p_2}{q_2}\right),$$

что и требовалось доказать.

В частности, последовательность чисел $\{3^n\}$, $n \in N$, которая образуется в пирамиде Паскаля при $\frac{p_1}{q_1} = \frac{p_2}{q_2} = 0$, представляет собой числа различных полных покрытий прямоугольника размера $1 \times n$ квадратами трех разных цветов размера 1×1.

Последовательность чисел Якобсталя [5] 1, 3, 5, 11, 21, 43, 85, 171, 341, 683, 1365, ..., которая образуется в пирамиде Паскаля при $\frac{p_1}{q_1} = \frac{p_2}{q_2} = 1$, представляет собой числа различных полных покрытий прямоугольника размера $1 \times n$ квадратами размера 1×1 и прямоугольниками двух разных цветов размера 1×2.

Последовательность чисел Трибоначчи [1] 1, 1, 2, 4, 7, 13, 24, 44, 81, 149, 274, 504, ..., которая образуется в пирамиде Паскаля при $\frac{p_1}{q_1} = 2$, $\frac{p_2}{q_2} = 1$, или при $\frac{p_1}{q_1} = 1$, $\frac{p_2}{q_2} = 2$, представляет собой числа различных полных покрытий прямоугольника размера $1 \times n$ квадратами размера 1×1 и прямоугольниками размера 1×2 и 1×3.

Последовательность чисел Пелля [1] 1, 2, 5, 12, 29, 70, 169, 408, 985, 2378, ..., которая образуется в пирамиде Паскаля при $\frac{p_1}{q_1} = \frac{p_2}{q_2} = -\frac{1}{2}$, представляет собой числа различных полных покрытий прямоугольника размера $1 \times n$ прямоугольниками размера 1×2 и квадратами двух разных цветов размера 1×1.

Список литературы

1. Кузьмин О. В. Обобщенные пирамиды Паскаля и их приложения. — Новосибирск: Наука. Сибирская издательская фирма РАН, 2000.

2. Серёгина М. В. Некоторые плоские сечения пирамиды Паскаля // Ресурсосберегающие технологии на транспорте и в промышленности: сб. научн. тр. — Чита: ЗабИЖТ, 2007. — С. 188–194.

3. Серёгина М. В. Некоторые плоские сечения А- и В-пирамид // Моделирование. Системный анализ. Технологии: межвузовский сборник научных трудов. — Чита: ЗабИЖТ, 2008. — С. 24–35.

4. Серёгина М. В. Некоторые восходящие диагональные сечения пирамиды Паскаля и покрытия прямоугольников // Вестник Иркутского университета: Ежегодная научно-теоретическая конференция аспирантов и студентов: материалы. — Иркутск: Изд-во Иркут. гос. ун-та, 2009. — С. 164–166.

5. Cerin Z. Sums of squares and products of Jacobsthal numbers // Journal of Integer Sequences. — 2007. — V. 10, Article 07.2.5.

ОБ АНАЛИЗЕ ИНФОРМАЦИИ

В. К. Леонтьев (Москва)

Под анализом информации обычно подразумевается извлечение "полезных" данных из текста, в котором эти данные представлены косвенным, искаженным или недостаточно полным образом. Такой анализ является необходимым во многих содержательных ситуациях, связанных с восстановлением поврежденных текстов, сравнением генетических последовательностей, автоматическим переводом с одного языка на другой и т. д.

Мы рассматриваем одну из возможных моделей, связанных с анализом информации. В целом ряде работ эта модель известна как "восстановление слов по фрагментам". Исходным объектом является слово. Это слово представлено некоторым набором своих "частей". Требуется путем анализа этих частей расшифровать исходное слово с той точностью, которую допускает исходная информация. Под "точностью" в содержательном смысле понимается множество всех "кандидатов" на роль неизвестного слова.

В этой работе мы для расшифровки неизвестного слова используем также априорную информацию, т. е. то семейство слов, которому заведомо принадлежит предмет поиска. Такая априорная информация может иметь различную форму: предикатное описание, набор признаков, "геометрическое расположение" и т. д.

Пусть $I_n = \{1, 2, \ldots, n\}$ и $v \subseteq I_n$. Тогда при $x = (x_1, \ldots, x_n)$ по определению полагаем

$$x_v = x_{i_1} x_{i_2} \ldots x_{i_k},$$

где $v = (i_1, i_2, \ldots, i_k)$.

Пусть $V = \{v_1, \ldots, v_N\}$, где $v_i \subseteq I_n$. Множество V называется характеристическим.

Определение. Слова $x, y \in B^n$ называются V-*эквивалентными*, если выполняется соотношение

$$\{x_{v_i}\} = \{y_{v_i}\}, \tag{1}$$

где равенство (1) понимается как равенство двух мультимножеств. Каждое из слов x_{v_k} называется фрагментом x.

Описание класса эквивалентности V_a может быть дано в форме множества единиц некоторой булевой функции, заданной как логический перманент булевой матрицы, построенной по характеристическому множеству V и слову $a \in B^n$. Аналогичным образом строится класс эквивалентности слова a при априорной информации $a \in A$.

Пусть $T(x)$ — преобразование циклического сдвига, т. е.

$$T(x_1, \ldots, x_n) = (x_n, x_1, \ldots, x_{n-1}).$$

Рассмотрим транзитивное множество или траекторию

$$a_T = \{a, Ta, T^2a, , \ldots\}.$$

Будем считать априорной информацией о неизвестном слове x принадлежность траектории a_T.

Теорема. *Если $x \in a_T$, $\|a\| = m$ и $(m, n) = 1$, то любое слово $x \in a_T$ однозначно определяется фрагментами длины два.*

В работе рассматриваются также другие примеры использования априорной информации для восстановления слов по набору их фрагментов.

Работа выполнена при финансовой поддержке РФФИ, проект 08–01–00414.

СУЩЕСТВОВАНИЕ ПРОСТЫХ МАТРИЦ НАД ДИСТРИБУТИВНЫМИ РЕШЕТКАМИ

В. Е. Маренич (Москва)

Наиболее известны простые матрицы над двухэлементной булевой решеткой $P = \{\widetilde{0}, \widetilde{1}\}$, которые изучались в работах [1–10]. Свойства простых $\{\widetilde{0}, \widetilde{1}\}$ — булевых матриц рассматривались в книгах [11, 12].

Первым вопросом, возникающим при изучении простых решеточных матриц, является вопрос о существовании простых матриц над данной дистрибутивной решеткой.

Пусть $(P, \wedge, \vee, \leq)$ — дистрибутивная решетка с нулем $\widetilde{0}$ и единицей $\widetilde{1}$. *Решеточными матрицами* будем называть матрицы, элементы которых принадлежат множеству P. Обозначим $P^{m\times n}$ множество всех решеточных матриц размера $m \times n$, где числа $n, m \geq 1$.

Единичная матрица $E_{n\times n} = (e_{ij})_{n\times n} \in P^{n\times n}$ определена равенствами

$$e_{ij} = \begin{cases} \widetilde{1}, & i = j, \\ \widetilde{0}, & i \neq j. \end{cases}$$

Матрица размера $m \times n$, все элементы которой равны нулю $\widetilde{0}$, называется *нулевой* и обозначается $0_{m\times n}$.

Если каждый элемент матрицы $A \in P^{m\times n}$ имеет дополнение, то матрица $\overline{A} \in P^{m\times n}$, где $\overline{a}_{ij} = \overline{a_{ij}}$ для всех $i = 1, \ldots, m$, $j = 1, \ldots, n$, называется *матрицей дополнений*.

Сложение и умножение матриц над решеткой $(P, \wedge, \vee, \leq)$ определяются как обычно: вместо операции сложения используется операция объединения $\vee$, а вместо операции умножения используется операция пересечения $\wedge$.

Пусть матрица $A \in P^{n\times n}$. Матрица A называется *обратимой слева* (или *справа*), если существует матрица $B \in P^{n\times n}$ такая, что $BA = E_{n\times n}$ (или $AB = E_{n\times n}$).

Элементарная матрица $El_n(k, \lambda)$ *первого вида* — это матрица, полученная из единичной матрицы $E = E_{n\times n}$ заменой столбца $E^{(k)}$ на столбец $\lambda E^{(k)}$. *Элементарная матрица* $El_n(k, l, \lambda)$ *второго вида* — это матрица, полученная из единичной матрицы E заменой столбца $E^{(k)}$ на столбец $E^{(k)} + \lambda E^{(l)}$, где $k \neq l$.

Строчечным пространством матрицы A называется линейная оболочка векторов-строк матрицы A. *Столбцовым пространством* матрицы A называется линейная оболочка векторов-столбцов матрицы A. Строчечные и столбцовые пространства матрицы A обозначаются, соответственно, $Row(A)$ и $Column(A)$.

Матрица A называется *простой над решеткой* $(P, \wedge, \vee, \leq)$ (или *простой матрицей моноида* $P^{n\times n}$), если она не обратима и из равенства $A = BC$, где $B, C \in P^{n\times n}$, следует, что B или C – обратимая матрица.

Необратимая матрица A называется *факторизуемой*, если $A = BC$, где необратимые матрицы $B, C \in P^{n\times n}$. Разложение $A = BC$ называется *факторизацией матрицы* A.

Если в дистрибутивной решетке $(L, \wedge, \vee, \leq)$ дополнение имеют не только нуль $\widetilde{0}$ и единица $\widetilde{1}$, то матрица $\overline{E}_{n\times n}$ факторизуема для всех $n \geq 3$.

Определим *множество подпространств*

$$Space_{n\times n}(P) = \{Column(Z) | Z \in P^{n\times n}\}.$$

Множество $Space_{n\times n}(P)$ состоит из подпространств пространства $P^{n\times 1}$, размерность которых не превосходит числа n.

Теорема 1. *Пусть матрица $A \in P^{n\times n}$. Если A — простая матрица, то пространства $Column(A)$ и $Column({}^tA)$ являются коатомами частично упорядоченного множества $(Space_{n\times n}(P), \subseteq)$.*

Теорема 2. *Пусть V — подпространство пространства $P^{n\times 1}$. Если подпространство V — коатом частично упорядоченного множества $(Space_{n\times n}(P), \subseteq)$, то справедливо одно из следующих утверждений.*
i) $V = Column(A)$, где простая матрица $A \in P^{n\times n}$.
ii) $V = Column(El_n(k, l, \alpha))$, где числа $k, l = 1, \ldots, n$, $k \neq l$ и α — атом решетки $(P, \wedge, \vee, \leq)$.
iii) $V = Column(El_n(k, \eta))$, где число $k = 1, \ldots, n$ и η — коатом решетки $(P, \wedge, \vee, \leq)$, $\eta > \widetilde{0}$.

Теорема 3. *Пусть числа $k, l, m = 1, \ldots, n$, $k \neq l$.*
Тогда пространства
- *$V_1 = Column(A)$, где простая матрица $A \in P^{n\times n}$,*
- *$V_2 = Column(El_n(k, l, \alpha))$, где α – атом решетки $(P, \wedge, \vee, \leq)$,*
- *$V_3 = Column(El_n(m, \eta))$, где η – коатом решетки $(P, \wedge, \vee, \leq)$, $\eta > \widetilde{0}$,*

попарно различны.

Теорема 4. *Над решеткой $(P, \wedge, \vee, \leq)$ не существует простых 2×2 решеточных матриц.*

Рассмотрим критерий существования простых матриц.

Теорема 5. *Пусть каждое пространство, принадлежащее множеству $Space_{n\times n}(P)$ и отличное от пространства $P^{n\times 1}$, содержится в некоторых коатомах ЧУМ $(Space_{n\times n}(P), \subseteq)$. Тогда над решеткой $(P, \wedge, \vee, \leq)$ существуют простые $n\times n$ матрицы, для всех $n \geq 3$.*

Следствие 1. *Пусть $(P, \wedge, \vee, \leq)$ — конечная дистрибутивная решетка, $|P| \geq 2$. Тогда над решеткой $(P, \wedge, \vee, \leq)$ существуют простые $n \times n$ матрицы, для всех $n \geq 3$.*

Список литературы

1. Borosh J., Hartfiel D. J., Maxson C. J. Answer to questions posed by Richman and Shneider // Linear and Multilinear Algebra. — 1976. — V. 3. — P. 255–258.

2. de Caen D. Prime Boolean matrices // M.Sc. Thesis. — Queen's Univ., Kingston, Ontario, 1979.

3. de Caen D., Gregory D. A. Prime Boolean matrices // Combinatorial Mathematics Society of Australia. — Springer Lecture Notes in Mathematics. — Aug., 1979.

4. de Caen D., Gregory D. A. Primes in the semigroup of Boolean matrices // Linear Algebra and its Applications. — 1981. — V. 37. — P. 119–134.

5. Richman D. J., Schneider H. Primes in the semigroup of nonnegative matrices // Linear and Multilinear Algebra. — 1974. — V. 2. — P. 135–140.

6. Tchunte M. On the Decomposition of Boolean Matrices // Lecture Note. — Univ. of Grenoble, Grenoble, France,1980.

7. Gregory D. A., Pullman N. J. Prime Boolean matrices, a graph theoretic approach // Ars Combinatoria. — 1981. — V. 12. — P. 81–110.

8. Gregory D. A., Pullman N. J. Semiring rank: Boolean rank and nonnegative rank factorization // Journal of Combinatorics, Information & System Sciences. — 1983. — V. 8, № 3. — P. 223–233.

9. Han Hyun Cho. Prime Boolean matrices and factorizations // Linear Algebra Appl. — 1993. — V. 190. — P. 87–98.

10. Han Hyun Cho. Permanents of prime Boolean matrices // Bull. Korean Math. Soc. — 1998. — V. 35, № 3. — P. 605–613.

11. Kim Ki Hang. Boolean matrix theory and applications // Marcel Dekker, New York, 1982.

12. Сачков В. Н., Тараканов В. Е. Комбинаторика неотрицательных матриц. — М.: ТВП, 2000.

КВАЗИПОРЯДКОВАЯ РАЗМЕРНОСТЬ ДВУДОЛЬНЫХ ЧАСТИЧНЫХ ПОРЯДКОВ

Е. Е. Маренич (Мурманск)

Пусть (P, T) — конечное квазиупорядоченное множество (КУМ).

Квазипорядковая размерность $\dim_q(T) = \dim_q(P, T)$ квазипорядка (КП) T определена в работе [1] как наименьшее число коатомов решетки квазипорядков $Qord(P)$, пересечение которых равно T. *Квазипорядковая размерность* $\dim_q(T)$ частичного порядка (ЧП) T

совпадает с размерностью $\dim_2(T)$, определенной Троттером [2 3], и равна наименьшему числу n такому, что ЧП T вложим в решетку подмножеств n-элементного множества. Свойства квазипорядковой размерности частично упорядоченных множеств (ЧУМ) рассмотрены в работах [1–3]. В работе рассматриваются только конечные КП и ЧП.

Коатомы γ решетки $Qord(P)$ называют *гантелями*, и изображают дробями $\gamma = \frac{U(\gamma)}{D(\gamma)}$, где $U(\gamma) \neq \emptyset$, $D(\gamma) \neq \emptyset$, $U(\gamma) \cap D(\gamma) = \emptyset$, $U(\gamma) \cup D(\gamma) = P$. При этом $a\gamma b$ равносильно $a, b \in U(\gamma)$ или $a, b \in D(\gamma)$, или $a \in D(\gamma), b \in U(\gamma)$.

Если Z — множество коатомов решетки $Qord(P)$, пересечение которых равно Q, то будем говорить, что семейство Z *реализует* Q. Если $|Z| = \dim_q(Q)$ и Z реализует Q, то назовем Z *наименьшей квазипорядковой реализацией* Q.

Рассмотрим множества $A = \{a_1, \ldots, a_{n+k}\}$, $B = \{b_1, \ldots, b_{n+k}\}$ такие, что $|A| = |B| = n + k$, $A \cap B = \emptyset$, где числа $n \in N$, $k \in N_0$. Определим частичноупорядоченное множество (ЧУМ) $S_n^k = (P, \leq)$ следующим образом: 1) диаграммой Хассе ЧУМ является двудольный граф с нижней долей A и верхней долей B; 2) неравенство $a_i < b_j$ равносильно тому, что $i = j + k + 1, j + k + 2, \ldots, j + k + n - 1$, (или $i \neq j, j + 1, \ldots, j + k$), где сложение производится по модулю $n + k$.

В дальнейшем ЧП $\leq$ будем обозначать S_n^k.

В работах Троттера [2, 3] *обобщенные короны* определены как ЧП S_n^k, где $n \geq 3$, $k \geq 0$. Обобщенные короны S_n^0, $n \geq 3$, называют *коронами*. В работе [2] для обобщенных корон было доказано, что

$$\dim_q(S_n^k) = k + n. \tag{1}$$

Позднее [3, стр. 249] было замечено, что формула (1), вообще говоря, ошибочна. В данной работе формула (1) доказана для всех $n \geq 3$, $k \geq 0$, $n > k$. Вычислена квазипорядковая размерность прямой суммы $S_n^0 + T$, $n \geq 3$, где T — нетривиальный ЧП такой, что $\dim_q(T) \leq n$. Доказано, что $\dim_q(S_n^0 + T) = n + 2$. В частности, $\dim_q(S_n^0 + S_n^0) = n + 2$.

Прямая сумма (дизъюнктивное объединение) частичных порядков T_1 и T_2 обозначается $T_1 + T_2$ [4, стр. 153]. Прямая сумма n одинаковых ЧП T обозначается nT. Порядковая сумма частичных порядков T_1 и T_2 обозначается $T_1 \oplus T_2$, см. [4, стр. 153]. Порядковая сумма n одинаковых ЧП T обозначается $\oplus nT$.

ЧП θ, определенный на одноэлементном множестве, будем называть *тривиальным*.

ЧП $\leq$ на множестве P называется *двудольным*, если $P = A \cup B$, где $A \neq \emptyset$, $B \neq \emptyset$, $A \cap B = \emptyset$, и для любых $a, b \in P$ из условия $a < b$ следует, что $a \in A$, $b \in B$. Диаграммой Хассе двудольного ЧП $\leq$ является двудольный граф $\Gamma = \Gamma(A \cup B, E)$ с долями A, B и множеством ребер $E = \{\{a, b\} \mid a \in A,\ b \in B,\ a < b\}$. Определим функции $\varphi : A \to 2^B$ и $\psi : B \to 2^A$ равенствами

$$\varphi(a) = \{z | z \in B, a < z\},\ a \in A; \qquad \psi(b) = \{u | u \in A, u < b\},\ b \in B.$$

Двудольный граф Γ определяет двудольный граф $\overline{\Gamma} = \Gamma(A \cup B, \overline{E})$, где $\overline{E} = \{\{a, b\} \mid a \in A,\ b \in B\} - E$. *Паросочетанием из доли A в долю B* графа $\overline{\Gamma}$ называется инъекция $\chi : A \to B$ такая, что $\{a, \chi(a)\} \in \bar{E}$.

При вычислении квазипорядковой размерности некоторых двудольных ЧП полезна следующая лемма.

Лемма 1. *Пусть $\leq$ — двудольный ЧП, диаграммой Хассе которого является двудольный граф $\Gamma = \Gamma(A \cup B, E)$, имеющий следующие свойства*: 1. $|\psi(z)| \geq 2$ *для всех* $z \in B$. 2. *Если* $\psi(z) \subseteq \psi(v)$, *то* $z = v$ *для любых* $z, v \in B$. 3. *Существует такое паросочетание χ из доли A в долю B графа $\overline{\Gamma}$, что для всех $z \in A$ справедливо равенство $\chi(\overline{\psi(\chi(z))} \cap \overline{\varphi(z)} = \{\chi(z)\}$, где $\overline{\psi(\chi(z))} = A - \psi(\chi(z))$, $\overline{\varphi(z)} = B - \varphi(z)$.*

Тогда справедливы следующие утверждения.

i) Для каждой вершины $z \in A$ в каждой реализации Z частичного порядка $\leq$, существует такая гантель γ, что $\{z\} \cup \varphi(z) \subseteq U(\gamma)$ и $\{\chi(z)\} \cup \psi(\chi(z)) \subseteq D(\gamma)$. *ii)* $\dim_q(\leq) = |A|$.

Теорема 1. *Для всех $n \geq 3$, $k \geq 0$, $n > k$, справедливо равенство*

$$\dim_q(S_n^k) = n + k.$$

Следствие 1. *Для всех $n \geq 3$ справедливы утверждения*:

i) $\dim_q(S_n^0) = n$.

ii) Каждая квазипорядковая реализация короны S_n^0 содержит гантели

$$\frac{\{a_i\} \cup (B - \{b_i\})}{\{b_i\} \cup (A - \{a_i\})},\ i = 1, 2, \ldots, n. \tag{2}$$

iii) Существует единственная наименьшая квазипорядковая реализация короны S_n^0. Гантели этой реализации заданы (2).

Теорема 2. *Пусть $n \geq 3$. Справедливы утверждения.*

i) $\dim_q(S_n^0 + \theta) = n + 1$.

ii) *Существует только две наименьшие квазипорядковые реализации прямой суммы* $S_n^0 + \theta$. *Гантели этих реализаций заданы равенствами* (3)

$$\gamma_i = \frac{\{a_i\} \cup (B - \{b_i\}) \cup \{u\}}{\{b_i\} \cup (A - \{a_i\})}, \quad i = 1, 2, \ldots, n; \quad \gamma_{n+1} = \frac{A \cup B}{\{u\}}, \quad (3)$$

или равенствами (4)

$$\gamma_i = \frac{\{a_i\} \cup (B - \{b_i\})}{\{b_i\} \cup (A - \{a_i\}) \cup \{u\}}, \quad i = 1, 2, \ldots, n; \quad \gamma_{n+1} = \frac{\{u\}}{A \cup B}. \quad (4)$$

Теорема 3. *Если* $n \geq 3$, *то* $\dim_q(S_n^0 + (\theta + \theta)) = n + 2$.

Теорема 4. *Если* $n \geq 3$, *то* $\dim_q(S_n^0 + (\theta \oplus \theta)) = n + 2$.

Следствие 2. *Если* $n \geq 3$, *то* $\dim_q(S_n^0 + T) = n + 2$, *где* T *не тривиальный ЧП такой, что* $\dim_q(T) \leq n$. *В частности,* $\dim_q(S_n^0 + S_n^0) = n + 2$.

Пусть множество $U = \{1, 2, \ldots, n\}$, $n \geq 4$, $0 \leq k < l \leq n$. Уровневые множества булеана $Bul(n)$ определены равенствами

$$W_r = \{z | z \subseteq U, |z| = r\}, \quad r = 0, 1, \ldots, n.$$

Определим двудольный ЧП $T_{n,k,l}$, $k \neq l$, на множестве $W_k \cup W_l$, где $aT_{n,k,l}b$ равносильно $a \subseteq b$. Диаграммой Хассе ЧП $T_{n,k,l}$ является регулярный двудольный граф $\Gamma_{n,k,l} = \Gamma(W_k \cup W_l, E)$, где $E = \{\{a, b\} | a \in W_k, b \in W_l, a \subseteq b\}$.

Теорема 5. Если $n \geq 4$, то $\dim_q(T_{n,1,n-2}) = n$.

Следствие 3. Если $n \geq 4$, то $\dim_q(T_{n,2,n-1}) = n$.

Список литературы

1. Филимонов В. Ю. Квазипорядковая размерность квазиупорядоченных множеств // В печати.

2. Trotter W. T. Embedding finite posets in cubes // Discrete Math. — 1975. — V. 12. — С. 165–172.

3. Trotter W. T. Combinatorics and partially ordered sets: dimension theory // Baltimore and London: The Johns Hopkins University Press, 1992.

О ПАРАСТРОФНО-ОРТОГОНАЛЬНЫХ КВАЗИГРУППАХ И ГРАФАХ

Т. В. Попович (Кишинев)

Понятие ортогональности играет важную роль в теории латинских квадратов, в теории квазигрупп и в различных приложениях, в частности в теории кодирования и криптографии. При этом значительный интерес представляют квазигруппы, ортогональные некоторым их парастрофам, или два парастрофа которых ортогональны (известные как сопряженно-ортогональные или парастрофно-ортогональные квазигруппы).

Квазигруппа — это упорядоченная пара (Q, A), где Q — множество, а A — бинарная операция, определенная на Q, и такая, что каждое из уравнений $A(a, y) = b$ и $A(x, a) = b$ однозначно разрешимо для любой пары элементов a, b из Q. Квазигруппа (Q, A) называется *T-квазигруппой*, если существуют абелева группа $(Q, +)$, ее автоморфизмы φ, ψ и элемент $c \in Q$ такие, что $A(x, y) = \varphi x + \psi y + c$ для любых $x, y \in Q$ [1].

Известно, что таблица умножения конечной квазигруппы определяет латинский квадрат и что с каждой квазигруппой (латинским квадратом) связана система из шести (не обязательно различных) сопряженных операций или парастрофов [2]: A, ${}^{r}A$, ${}^{l}A$, ${}^{rl}A$, ${}^{lr}A$, ${}^{s}A$, где ${}^{r}A(x, y) = z \Leftrightarrow A(x, z) = y$, ${}^{l}A(x, y) = z \Leftrightarrow A(z, y) = x$ и ${}^{s}A(x, y) = A(y, x)$, которые также квазигруппы (${}^{rl}A = {}^{r}({}^{l}A)$). Число различных парастрофов в Σ может быть 1,2,3 или 6 [3].

Две квазигруппы (Q, A) и (Q, B) ортогональны, если система уравнений $\{A(x, y) = a,\ B(x, y) = b\}$ однозначно разрешима для всех элементов a, b из Q.

Множество $\Sigma = \{A_1, A_2, ..., A_t\}$, $t \geq 2$, квазигрупп, определенных на одном и том же множестве, ортогонально, если любые две квазигруппы этого множества ортогональны.

Граф ортогональности латинских квадратов — это граф, вершинами которого являются латинские квадраты одинакового порядка из одних и тех же символов, а две вершины являются смежными тогда и только тогда, когда латинские квадраты ортогональны. В статье [4] рассматривается представление ортогональных связей парастрофов латинского квадрата L графом, в котором вершинами являются парастрофы, а две вершины соединены тогда и только тогда, когда соответствующие парастрофы ортогональны. Такой граф называется графом сопряженной (парастрофной) ортогональности латинского квадрата L. Проблема описания полного спектра

латинских квадратов, реализующих полный граф K_6 сопряженной ортогональности латинского квадрата, еще остается открытой.

В [5] Беннет доказал, что идемпотентные латинские квадраты со всеми различными и попарно ортогональными парастрофами существуют любого порядка $n > 5074$. В [2] Белоусов показал, что существуют бесконечные квазигруппы, все парастрофы которых попарно ортогональны, и привел пример такой квазигруппы.

В [6] аннонсированы результаты о спектре квазигрупп, все парастрофы которых различны и попарно ортогональны (такие квазигруппы названы *тотально парастрофно-ортогональными*, сокращенно, *totCO-квазигруппами*), и приведены следующие необходимые и достаточные условия, чтобы T-квазигруппа была $totCO$-квазигруппой.

Пусть $\sigma \perp \tau$ означает, что ${}^{\sigma}A \perp^{\tau} A$, в $\sigma\tau$ сначала берется парастроф τ, затем парастроф σ, $(\varphi+\psi)x = \varphi x + \psi x$, а ε является тождественной подстановкой. Очевидно, что если ${}^{\sigma}A \perp^{\tau} A$, то ${}^{s\sigma}A \perp^{s\tau} A$.

Теорема 1. *T-Квазигруппа (Q, A): $A(x, y) = \varphi x+\psi y+c$ является totCO-квазигруппой тогда и только тогда, когда все отображения $\varphi+\varepsilon$, $\varphi-\varepsilon$, $\psi+\varepsilon$, $\psi-\varepsilon$, $\varphi^2+\psi$, $\psi^2+\varphi$, $\varphi-\psi$, $\varphi+\psi$, $\psi\varphi-\varepsilon$ являются подстановками.*

С помощью этого результата доказано, что для любого целого числа $n \geq 11$, взаимно простого с 2,3,5 и 7, существует $totCO$-квазигруппа порядка n.

Любая конечная $totCO$-квазигруппа соответствует полному графу K_6 сопряженной ортогональности латинского квадрата, поэтому из предыдущего результата следует аналогичная информация относительно спектра латинских квадратов, реализующих полный граф K_6 сопряженной ортогональности.

Квазигруппу (Q, A) назовем *почти тотально парастрофно-ортогональной* или *почти totCO-квазигруппой*, если хотя бы пять из шести ее парастрофов образуют ортогональное множество. В этом случае все шесть парастрофов различны.

Теорема 2. *Если квазигруппа не является totCO-квазигруппой, то множества $\Sigma_1 = \{l, r, rl, lr, s\}$, $\Sigma_s = \{1, r, l, rl, lr\}$ ее парастрофов ортогональны тогда и только тогда, когда все пары парастрофов, кроме пары $(1, s)$, ортогональны; множества $\Sigma_l = \{1, r, rl, lr, s\}$, $\Sigma_{lr} = \{1, r, l, rl, s\}$ ее парастрофов ортогональны тогда и только тогда, когда все пары парастрофов, кроме пары (l, lr), ортогональны; множества $\Sigma_r = \{1, l, rl, lr, s\}$, $\Sigma_{rl} = \{1, r, l, lr, s\}$ ее парастрофов ортогональны тогда и только тогда, когда все пары парастрофов, кроме пары (r, rl), ортогональны.*

Назовем граф парастрофной ортогональности квазигруппы *почти полным*, если он содержит не менее четырнадцати ребер.

Следствие 1. *Любой почти totCO-квазигруппе соответствует почти полный граф парастрофной ортогональности.*

Теорема 3. *T-Квазигруппа (Q, A): $A(x, y) = \varphi x + \psi y + c$, не являющаяся totCO-квазигруппой, является почти totCO-квазигруппой тогда и только тогда, когда из всех отображений теоремы* 1 *только единственное отображение $\varphi - \varepsilon$ ($\psi - \varepsilon$ или $\varphi + \psi$) не является подстановкой.*

Для каждой отсутствующей пары парастрофов из теоремы 2 приведены примеры T-квазигрупп, являющихся почти *totCO*-квазигруппами (но не *totCO*-квазигруппами), а следовательно, реализующих почти полный граф парастрофной ортогональности, который не является полным.

Список литературы

1. Kepka T., Nemec P. T-quasigroups. I // Acta Universitatis. Carolinae. Math. et Phys. — 1971. — V. 12, № 1. — P. 39–49.

2. Belousov V. D. Parastrophic-orthogonal quasigroups // Quasigroups and related systems. —2005. — V. 13, № 1. — P. 25–73.

3. Lindner C. C., Steedly D. On the number of conjugates of a quasigroup // Algebra Univ. —1975. — № 5. — P. 191–196.

4. Lindner C. C., Mendelsohn E., Mendelsohn N. S., Wolk B. Orthogonal Latin square graphs // J. Graph Theory. — 1973. — № 3. — P. 325–328.

5. Bennett F. E. On conjugate orthogonal idempotent Latin squares // Ars. combinatorica. —1985. — № 19. — P. 37–50.

6. Belyavskaya G., Popovich T. Totally conjugate-orthogonal quasigroups // Abstracts of the 7-th International Algebraic Conference in Ukraine (Kharkov, 18–23 August, 2009). — P. 26–27.

О ЧИСЛЕ КЛИКОСОЧЕТАНИЙ В k-ЗНАЧНОМ ГИПЕРКУБЕ

В. Н. Потапов (Новосибирск)

Пусть $Q_k = \{0, \ldots, k-1\}$. *k-Значным n-мерным кубом* (*гиперкубом*) называется множество Q_k^n. Гиперкубом называют также граф ΓQ_k^n минимальных расстояний метрического пространства (Q_k^n, d),

где d — расстояние Хэмминга. Одномерная грань направления i, проходящая через вершину $(a_1, \ldots, a_n) \in Q_k^n$, определяется как

$$(a_1, \ldots, a_{i-1}, \mathbf{x}, a_{i+1}, \ldots, a_n) = \{(a_1, \ldots, a_{i-1}, x, a_{i+1}, \ldots, a_n) : x \in Q_k\}$$

и является максимальной кликой в гиперкубе ΓQ_k^n. Множество одномерных граней в гиперкубе Q_k^n будем обозначать через $\widetilde{Q}_k^n$. Элементы множества $\widetilde{Q}_k^n$ удобно рассматривать как слова в алфавите $Q_k \cup \{\mathbf{x}\}$. *Кликосочетанием* в Q_k^n будем называть набор не пересекающихся одномерных граней (клик). При $k = 2$ понятие кликосочетания в Q_2^n совпадает с понятием паросочетания.

Кликосочетание B в гиперкубе Q_k^n будем называть *совершенным*, если оно является разбиением вершин гиперкуба на одномерные грани, т. е. $Q_k^n = \bigcup\limits_{b \in B} b$. Ясно, что кликосочетание $B \subset \widetilde{Q}_k^n$ является совершенным тогда и только тогда, когда $|B| = k^{n-1}$. Здесь и далее через $|A|$ обозначается мощность множества A.

Кликосочетание можно рассматривать как функцию, ставящую в соответствие каждой вершине из Q_k^n направление i одномерной грани кликосочетания, в которой лежит вершина, или 0, если вершина не содержится ни в одной грани кликосочетания. Нетрудно видеть, что функция $f : Q_k^n \to \{0, 1, \ldots, n\}$ определяет кликосочетание, если удовлетворяет следующему условию

$$f(a_1, ., a_{i-1}, a_i, a_{i+1}, ., a_n) = i \neq 0 \;\Rightarrow$$

$$\forall x \in Q_k \; f(a_1, ., a_{i-1}, x, a_{i+1}, ., a_n) = i.$$

В дальнейшем будем называть кликосочетанием и определяющую кликосочетание функцию. Кликосочетание f является совершенным тогда и только тогда, когда $0 \notin f(Q_k^n)$. Обозначим через $K_k(n)$ множество кликосочетаний в Q_k^n и через $SK_k(n)$ — множество совершенных кликосочетаний. В [3], как прямое следствие теорем из [1] и [2], указана асимптотика логарифма числа совершенных паросочетаний $\ln |SK_2(n)| = 2^{n-1}(\ln n - 1 + o(1))$ при $n \to \infty$. Целью настоящей работы является вычисление числа совершенных кликосочетаний.

Обозначим через $K_k(n, p)$ множество кликосочетаний, принимающих значение 0 с вероятностью p, т. е.

$$K_k(n, p) = \left\{ f \in K_k(n, p) \;:\; p = \frac{|\{x \in Q_k^n : f(x) = 0\}|}{k^n} \right\}.$$

Методом математической индукции по размерности n гиперкуба доказана следующая

Лемма. *Пусть* $0 < p < 1$ *и* $K_k(m,p) \neq \varnothing$ *для некоторого натурального* m. *Тогда* $|K_k(n,p)| \geq n^{ck^{n-1}(1+o(1))}$ *при* $n \to \infty$, *где* $c = p^{k-1}(1-p)\ln 2$.

Идея доказательства леммы состоит в следующем. Рассмотрим произвольную вектор-функцию $F \in (K_k(n,p))^k$, $F = (f_1, \ldots, f_k)$. Определим кликосочетание $g[F](x_1, x_2, \ldots, x_n, z) = f_z(x_1, x_2, \ldots, x_n)$. Часть нулевых значений $g[F]$ оказывается возможным заменить на значение $n+1$. Аккуратный подсчёт среднего числа возможностей таких замен приводит к рекуррентному соотношению, из которого получается требуемая асимптотическая оценка.

Теорема. $|SK_k(n)| \geq n^{c_n k^{n-3}}$ *при* $n \to \infty$, *где* $c_n = \frac{\ln 2(1+o(1))}{e}$.

Доказательство. Пусть $f \in K_k(n)$. Определим функцию

$$\widetilde{f}(x_1, \ldots, x_{n+1}) = \begin{cases} f(x_1, \ldots, x_n), & \text{если } f(x_1, \ldots, x_n) \neq 0, \\ n+1, & \text{если } f(x_1, \ldots, x_n) = 0. \end{cases}$$

Нетрудно видеть, что $\widetilde{f} \in SK_k(n)$. Тогда $|SK_k(n)| \geq |K_k(n-1,p)|$ для любого p, $0 < p < 1$. Выберем $p = 1 - \frac{1}{k}$. Тогда $p^{k-1} > 1/e$ и из леммы получаем требуемое неравенство.

Из функционального определения кликосочетания следует тривиальная верхняя оценка $|SK_k(n)| \leq n^{k^n}$ числа кликосочетаний в Q_k^n, поэтому справедливо

Следствие. $\ln |SK_k(n)| \asymp k^n \ln n$ *при* $n \to \infty$.

Работа выполнена при финансовой поддержке РФФИ, проект 08-01-00671.

Список литературы

1. Брэгман Л. М. Некоторые свойства неотрицательных матриц и их перманентов // Докл. АН СССР. — 1973. — Т. 211, № 1. — С. 27–30.

2. Егорычев Г. П. Доказательство гипотезы Ван дер Вардена для перманентов // Сиб. мат. журн. — 1981. — Т. 22, № 6. — С. 65–71.

3. Пережогин А. Л., Потапов В. Н. О числе гамильтоновых циклов в булевом кубе // Дискретн. анализ и исслед. операций. Сер. 1. — 2001. — Т. 8, № 2. — С. 52–62.

О ХАРАКТЕРИЗАЦИИ ТЕРНАРНЫХ МАТРОИДОВ

А. М. Ревякин (Москва)

Пусть $P(S)$ — множество всех подмножеств конечного множества S. Система $\mathcal{I} \subseteq P(S)$ подмножеств из S называется матроидом $M = (S, \mathcal{I})$, а множества из $\mathcal{I}$ — независимыми, если выполняются следующие условия: $\oslash \in \mathcal{I}$; если $A \subseteq B$ и $B \in \mathcal{I}$, то $A \in \mathcal{I}$; если $A, B \in \mathcal{I}$ и $|A| > |B|$, то найдется $a \in A \setminus B$ такое, что $B \cup \{a\} \in \mathcal{I}$. Подмножество A из S является зависимым, если $A \notin \mathcal{I}$. Максимальные по включению независимые множества называют базами, а минимальное по включению зависимые подмножества — циклами матроида.

Примеры матроидов.

1. Пусть S — n-элементное множество, k - некоторое целое такое, что $1 \leq k \leq n$, и $I = \{A \subseteq S : |A| \leq k\}$. Матроид (S, I) называют однородным и обозначают через $U_{k,n}$.

2. Пусть G — простой граф с множествами вершин V и ребер E. Тогда семейство всех циклов графа G является множеством всех циклов некоторого матроида $M(G)$ на E, называемого циклическим матроидом графа G. Матроид M называют графическим, если существует граф G, циклический матроид которого изоморфен M.

3. Пусть $S = \{1, 2, 3, 4, 5, 6, 7\}$, B — семейство, состоящее из всех подмножеств из S, содержащих 3 элемента, за исключением подмножеств $\{1, 2, 3\}$, $\{1, 4, 7\}$, $\{1, 5, 6\}$, $\{2, 4, 6\}$, $\{2, 5, 7\}$, $\{3, 4, 5\}$ и $\{3, 6, 7\}$. Тогда матроид Φ с семейством баз B на S называется матроидом Фано. Матроид Φ имеет 7 точек и 7 прямых: $\{1, 2, 3\}, \{1, 4, 7\}, \{1, 5, 6\}, \{3, 6, 7\}, \{3, 4, 5\}, \{2, 4, 6\}$. Матроид, получаемый из Φ заменой прямой $\{2, 4, 6\}$ на три тривиальные прямые $\{2, 4\}, \{2, 6\}$ и $\{4, 6\}$, обозначают через Φ^-.

4. Пусть $S = \{a_1, a_2, b_1, b_2, c_1, c_2, d_1, d_2\}$, B — семейство баз некоторого матроида, состоящее из всех подмножеств множества S, содержащих 4 элемента, за исключением подмножеств $\{a_1, a_2, b_1, b_2\}$, $\{a_1, a_2, c_1, c_2\}$, $\{b_1, b_2, d_1, d_2\}$, $\{c_1, c_2, d_1, d_2\}$ и $\{b_1, b_2, c_1, c_2\}$. Тогда (S, B) называют матроидом Вамоса.

Матроид M на множестве S называется представимым над полем F, если существует линейное пространство V над полем F и отображение $\phi : S \longrightarrow V$, при котором $A \subseteq S$ независимо в M тогда и только тогда, когда $\phi|_A$ взаимно однозначно и $\phi(A)$ — линейно независимое множество векторов в V.

Пусть $\mathrm{GF}(q)$ — конечное поле характеристики q. Матроид, представимый над полем $\mathrm{GF}(2)$ или $\mathrm{GF}(3)$, называют бинарным или тер-

нарным соответственно. Матроиды, представимые над каждым полем, называют унимодулярными (или регулярными). Матроид M является почти регулярным, если он может быть представлен над каждым полем, кроме поля GF(2). Известно, что Φ представим над полем $GF(2)$ и не представим ни над каким другим полем характеристики, отличной от 2. Матроид Φ^- является почти регулярным. Матроид Вамоса не представим ни над каким полем, а произвольный графический матроид является унимодулярным.

Многие проблемы теории матроидов касаются вопроса внутренней характеризации классов матроидов. Такие характеризации обычно получают в виде: "Существует некоторый минимальный, но возможно бесконечный, список $\mathcal{S}$ такой, что матроид M лежит в классе L тогда и только тогда, когда M не содержит миноров, изоморфных элементам из $\mathcal{S}$". Характеризации с помощью списка запрещенных миноров получены для большинства известных классов матроидов:

а) M является бинарным тогда и только тогда, когда никакой его минор не изоморфен $U_{2,4}$;

б) M является тернарным тогда и только тогда, когда не содержит миноров, изоморфных $U_{2,5}$, Φ, а также двойственным им;

в) M является унимодулярным тогда и только тогда, когда не содержит миноров, изоморфных $U_{2,4}$, Φ и двойственному ему Φ^*;

г) M является графическим тогда и только тогда, когда никакой его минор не изоморфен $U_{2,4}$, матроидам разрезов полных графов Куратовского K_5, $K_{3,3}$, Φ или двойственному ему Φ^*.

Характеристическое множество $Char(M)$ матроида M это такое множество $Char(M)$, что $p \in Char(M)$ тогда и только тогда, когда матроид M линейно представим над некоторым полем характеристики p .

Пусть множество Z состоит из всех положительных простых чисел и 0. Проблему координатизации матроидов можно сформулировать в следующем виде: "для каждого подмножества Q множества Z найти матроиды, которые линейно представимы над всеми полями с характеристиками из Q и не представимы ни над каким полем характеристики p, если $p \notin Q$".

У. Татт доказал, что если $p \neq 2$ и $\{2, p\} \subseteq Char(M)$, то $Char(M) = Z$. Поэтому представляют интерес вопросы представимости небинарных матроидов.

В докладе рассмотрены матроид Т. Брилавского и Д. Кэлли с $Char(M) = \{1103, 2089\}$, а также почти регулярные матроиды. Для класса почти регулярных матроидов получены новые матрич-

ные представления. Доказано, что матроид представим над полями $GF(3)$, $GF(4)$ и $GF(5)$ в том и только, в том случае, когда он является почти регулярным.

Матрица с рациональными коэффициентами называется двоичной, если все ее миноры равны 0 или $\pm 2^i$, где i — некоторое целое. Матроид, обладающий двоичной матрицей представления над полем рациональных чисел, называется двоичным. $\sqrt[6]{1}$-матрицей называется матрица с комплексными коэффициентами, все ненулевые миноры которой равны корням шестой степени из единицы. $\sqrt[6]{1}$-матроидом называется матроид, который можно представить столбцами $\sqrt[6]{1}$-матрицы.

Получены следующие результаты:

Теорема. *Матроид M является одновремено двоичным и $\sqrt[6]{1}$-матроидом тогда и только тогда, когда он принадлежит классу почти регулярных матроидов.*

Теорема. *Пусть M — тернарный матроид. Тогда для M справедливо одно из следующих утверждений:*

(i) *M представим только над полем характеристики три;*

(ii) *M — регулярный матроид;*

(iii) *M — почти регулярный матроид.*

Список литературы

1. Ревякин А. М. Координатизация и представимость матроидов // Комбинатор. анализ. Вып. 8. — М.: МГУ, 1989. – С. 6–37.

2. Whittle G. On matroids representable over GF(3) and other fields // Trans. Amer. Math. Soc. — 1997. — V. 349, № 2. — С. 579–603.

3. Revyakin A. M. On some classes of linear representable matroids // Formal Power Series and Algebraic Combinatorics: 12 International Conference; proceedings (FPSAC'00), Moscow, Russia, June 2000. – Berlin, N.Y.: Springer, 2000. — С. 564–574.

4. Oxley J. G. Matroid theory. —N.Y.: Oxford University Press, 2006.

ПОЛНОЦВЕТНЫЕ РАСКРАСКИ РАВНОМЕРНЫХ ГИПЕРГРАФОВ

А. П. Розовская, Д. А. Шабанов (Москва)

В работе исследуется известная задача экстремальной теории гиперграфов. Напомним, что *гиперграфом* называется пара множеств $H = (V, E)$, где $V = V(H)$ есть некоторое конечное множество,

называемое *множеством вершин* гиперграфа, а $E = E(H)$ есть совокупность каких-то подмножеств множества V, и эти подмножества называются *ребрами* гиперграфа. Гиперграф является *n-равномерным*, если каждое его ребро содержит ровно n вершин.

Раскраска множества вершин гиперграфа в r цветов (r-раскраска) называется *полноцветной* для H, если в ней каждое ребро из E содержит вершины всех цветов. В работе А. В. Косточки [1] была поставлена задача об отыскании величины $p(n, r)$, равной минимальному числу ребер гиперграфа в классе n-равномерных гиперграфов, не имеющих полноцветных r-раскрасок, т.е.

$p(n, r) = \min\{|E(H)|$: H — n-равномерный гиперграф, для которого не существует полноцветных r-раскрасок$\}$.

Задача об отыскании величины $p(n, r)$ хорошо известна в частном случае $r = 2$. В этом случае $p(n, 2)$ совпадает с классической величиной $m(n)$, равной минимальному числу ребер гиперграфа в классе n-равномерных гиперграфов, для которых не существует *правильных* двухцветных раскрасок (раскраска вершин гиперграфа называется правильной, если в этой раскраске все ребра гиперграфа являются неодноцветными). Проблема о нахождении $m(n)$ была поставлена в 1961 г. П. Эрдешем и А. Хайналом в работе [2]. Для $m(n)$ известны следующие оценки:

$$(\sqrt{3} - 1)\left(\frac{n}{\ln n}\right)^{\frac{1}{2}} 2^{n-1} \leq m(n) = p(n, 2) \leq \frac{e \ln 2}{2} n^2 2^{n-1}(1 + o(1)). \quad (1)$$

Верхнюю оценку впервые доказал П. Эрдеш [3]), нижнюю — Дж. Радхакришнан и А. Сринивасан [4]. Данные оценки остаются наилучшими из известных на сегодняшний день.

Одно из первых достаточных условий существования полноцветной r-раскраски у n-равномерного гиперграфа было получено в 1973 г. П. Эрдешем и Л. Ловасом в работе [5], которые доказали следующую теорему.

Теорема 1. *Пусть $2 \leq r \leq n$ и H — n-равномерный гиперграф. Если каждое ребро гиперграфа H пересекает не более $r^{n-1}/(4(r-1)^n)$ других ребер, тогда для H существует полноцветная r-раскраска.*

Из теоремы 1 следует, что $p(n, r) \geq r^{n-1}/(4(r-1)^n)$, однако, совсем несложно показать, что выполнено более сильное неравенство

$$p(n, r) \geq \frac{r^{n-1}}{(r-1)^n} = \frac{1}{r}\left(\frac{r}{r-1}\right)^n. \quad (2)$$

Задача о нахождении $p(n,r)$ имеет тесную связь с задачей о предписанных раскрасках полных r-дольных графов. Опираясь на эту связь, Косточка получил [1] следующие оценки для $p(n,r)$:

$$\frac{1}{r}\, e^{c_1 n/r} \le p(n,r) \le r\, e^{c_2 n/r}, \tag{3}$$

где c_1 и c_2 — некоторые абсолютные положительные константы, причем $c_1 < 1$, а $c_2 > 4$.

Наконец, в работе [6] были обоснованы следующие оценки величины $p(n,r)$ в частном случае $r = 3$:

$$c\left(\frac{n}{\ln n}\right)^{1/3}\left(\frac{3}{2}\right)^n \le p(n,3) \le \frac{e\ln 3}{12}n^2\left(\frac{3}{2}\right)^n(1+o(1)), \tag{4}$$

где c — некоторая положительная константа.

Основными результатами данной работы являются новые асимптотические оценки величины $p(n,r)$. В теоремах 2 и 3 сформулированы обобщения оценок (4) на случай произвольного числа цветов.

Теорема 2. *Для любых $n \ge 2$, $r \ge 2$ выполняется неравенство*

$$p(n,r) \ge \frac{\sqrt{21}-3}{4r}\left(\frac{n}{(r-1)\ln n}\right)^{1/3}\left(\frac{r}{r-1}\right)^n. \tag{5}$$

Теорема 3. *Пусть задана функция $r = r(n)$, удовлетворяющая условию $r \ge 3$. Пусть, кроме того, функция $d = d(n) := r^3/n^2$ не превосходит некоторой положительной константы $c < 1/2$ при всех $n > n_0$. Тогда существует такая функция $\varphi = \varphi(n)$, зависящая от функции r и стремящаяся к единице при $n \to \infty$, что для всех $n \ge n_0$ выполняется неравенство*

$$p(n,r) \le \frac{1}{r}\left(\frac{r}{r-1}\right)^n e\,(\ln r)\,\frac{n^2+\sqrt{n^4+16n^3r(r-1)}}{4(r-1)}\varphi.$$

Полученные в теоремах 2 и 3 оценки $p(n,r)$ асимптотически улучшают предыдущие известные результаты (2) и (3), в случае, когда r относительно невелико по отношению к n (например, (5) улучшает (2) и (3) при $r = r(n) = o\,(n/\ln n)$).

Еще одним результатом работы является новая нижняя оценка величины $p(n,3)$, сформулированная в теореме 4.

Теорема 4. *Существует такая положительная константа c, что для всех $n \geq 3$ выполняется неравенство*

$$p(n,3) \geq c \left(\frac{n}{\ln n}\right)^{1/2} \left(\frac{3}{2}\right)^n.$$

Нетрудно видеть, что данный результат асимптотически улучшает предыдущий результат (4). Отметим также, что порядок роста полученной оценки соответствует наилучшей известной нижней оценки $p(n,2) = m(n)$ (см. (1)). В обоих случаях оценка имеет вид

$$const\ (n/\ln n)^{1/2} (r/(r-1))^n.$$

Работа выполнена при финансовой поддержке РФФИ (грант 09-01-00294) и частичной поддержке гранта Президента РФ МК–3429.2010.1.

Список литературы

1. Kostochka A. V. On a theorem by Erdős, Rubin and Taylor on choosability of complete bipartite graphs // Electronic Journal of Combinatorics. — 2002. — V. 9, № 1.

2. Erdős P., Hajnal A. On a property of families of sets // Acta Mathematica of the Academy of Sciences, Hungary. — 1961. — V. 12. — P. 87–123.

3. Erdős P. On a combinatorial problem, II // Acta Mathematica of the Academy of Sciences, Hungary. — 1964. — V. 15, № 3–4. — P. 445–447.

4. Radkakrishnan J., Srinivasan A. Improved bounds and algorithms for hypergraph two-coloring // Random Structures and Algorithms. — 2000. — V. 16, № 1. — P. 4–32.

5. Erdős P., Lovász L. Problems and results on 3-chromatic hypergraphs and some related questions // Infinite and Finite Sets, Colloquia Mathematica Societatis Janos Bolyai, North Holland, Amsterdam. — 1975. — V. 11. — P. 609–627.

6. Шабанов Д. А. Экстремальные задачи для раскрасок равномерных гиперграфов // Известия РАН. Серия математическая. — 2007. — Т. 71, вып. 6. — С. 183–222.

ОБ ОДНОМ ОБОБЩЕНИИ ЧИСЕЛ БЕРНУЛЛИ И ЭЙЛЕРА

А. А. Саранцев (Москва)

Будем рассматривать подстановки на множестве $\{0,\dots,N\}$ (т. е. его биекции в себя), где $N \in \mathbb{Z}_+$. Такая подстановка τ *возрастает* (*убывает*) на множестве $\{p,\dots,q\} \subseteq \{0,\dots,N\}$, если для всех $j = p,\dots,q-1$ выполнено $\tau(j) < \tau(j+1)$ ($\tau(j) > \tau(j+1)$).

Пусть $n \in \mathbb{N}$, $i_1, j_1, \dots, i_n, j_n \in \mathbb{Z}_+$, $N := i_1 + j_1 + \dots + i_n + j_n$. Число подстановок на $\{0,\dots,N\}$, возрастающих на $\{s''_{k-1},\dots,s'_k\}$ и убывающих на $\{s'_k,\dots,s''_k\}$ для $k = 1,\dots,n$, обозначим так: $\Omega(i_1, j_1, \dots, i_n, j_n)$. Здесь и далее $s'_k := i_1 + j_1 + \dots + i_k$, $s''_k := i_1 + j_1 + \dots + i_k + j_k$.

Если $j_n = 0$, то этот аргумент в этих обозначениях опускается. Будем считать, что Ω с нулевым числом аргументов равно 1.

Лемма 1. $\Omega(p) = 1$, $\Omega(p,q) = (p+q)!/(p!q!)$ *при* $p,q \in \mathbb{Z}_+$.

Похожая, но более частная задача уже известна — это *задача Андре*: найти $b_n := \Omega(1,\dots,1)$ ($n-1$ единиц в скобках). Если определить *числа Бернулли* B_n и *числа Эйлера* E_n как коэффициенты

$$\frac{x}{e^x - 1} = \sum_{n=0}^{+\infty} \frac{B_n}{n!} x^n, \quad \frac{1}{\operatorname{ch} x} = \sum_{n=0}^{+\infty} \frac{E_n}{n!} x^n,$$

то [1, гл. 3, §1]

$$b_{2n-1} = \frac{(-1)^{n-1}}{n} 2^{2n-1}(2^{2n}-1)B_{2n}, \quad b_{2n} = (-1)^n E_{2n}.$$

Таким образом, числа Ω служат обобщением как биномиальных коэффициентов (см. лемму 1), так и чисел Бернулли и Эйлера.

Теорема 1. *Для* $n, i_1, \dots, i_n \in \mathbb{N}$ $\Omega(i_1,\dots,i_n) = \Omega(i_1-1,\dots,i_n) + \Omega(i_1, i_2-1, i_3,\dots,i_n) + \dots + \Omega(i_1,\dots,i_n-1)$.

Рассмотрим производящую функцию

$$F_n(x_1,\dots,x_n) := \sum_{i_1=0}^{+\infty} \dots \sum_{i_n=0}^{+\infty} \Omega(i_1,\dots,i_n) x_1^{i_1} \dots x_n^{i_n}.$$

Неравенство $\Omega(i_1,\dots,i_n) \le (i_1 + \dots + i_n)!/(i_1! \dots i_n!)$ нетрудно вывести из теоремы 1. Отсюда следует, что этот ряд сходится (абсолютно) при $|x_1| + \dots + |x_n| < 1$. Функция F_n при любом n дробно-

рациональна, и можно вычислить ее при любом заданном n. Например:

$$F_3(x_1,x_2,x_3)=\frac{1-x_1-x_3}{(1-x_1)(1-x_3)(1-x_1-x_2-x_3)},$$

$$F_4(x_1,x_2,x_3,x_4)=\frac{1}{1-x_1-x_2-x_3-x_4}\times$$

$$\times\left(\frac{(1-x_1)(1-x_1-x_2-x_4)}{(1-x_1-x_2)(1-x_1-x_4)}+\frac{(1-x_4)(1-x_1-x_3-x_4)}{(1-x_1-x_4)(1-x_3-x_4)}-1\right).$$

Отсюда выводятся общие формулы для Ω с 3, 4 и более аргументами.

Можно ввести так называемые *экспоненциальные производящие функции*: если $\Omega'(i_1,\ldots,i_n):=\Omega(i_1,\ldots,i_n)/(i_1+\ldots+i_n+1)!$, то

$$G_n(x_1,\ldots,x_n):=\sum_{i_1=0}^{+\infty}\ldots\sum_{i_n=0}^{+\infty}\Omega'(i_1,\ldots,i_n)x_1^{i_1}\ldots x_n^{i_n}.$$

Обычно под этим термином подразумевают производящую функцию для $\Omega(i_1,\ldots,i_n)/(i_1!\ldots i_n!)$ — но это нам будет неудобно. $\Omega'(i_1,\ldots,i_n)$ — это вероятность выбрать среди подстановок на $\{0,\ldots,i_1+\ldots+i_n\}$ подстановку с нужными промежутками монотонности. Ряд G_n уже, очевидно, сходится (абсолютно) при всех значениях аргументов.

Теорема 2. *Для* $n,i_1,j_1,\ldots,i_n,j_n\in\mathbb{N}$, $N:=i_1+\ldots+j_n$

$$\Omega'(i_1,\ldots,j_n)=\frac{1}{N+1}\sum_{k=1}^{n}\Omega'(i_1,j_1,\ldots,i_k-1)\Omega'(j_k-1,\ldots,i_n,j_n),$$

$$\Omega'(i_1,\ldots,j_n)=\frac{1}{N+1}\sum_{k=0}^{n}\Omega'(i_1,j_1,\ldots,j_k-1)\Omega'(i_{k+1}-1,\ldots,i_n,j_n).$$

Аналогичные две теоремы легко вывести для нечетного числа аргументов у Ω'. Из этих четырех теорем можно вывести следующую.

Теорема 3. *Для* $n,i_1,\ldots,i_n\in\mathbb{N}$, *если* $N:=i_1+\ldots+i_n$, *то*

$$\Omega'(i_1,\ldots,i_n)=\frac{1}{2(N+1)}\sum_{k=0}^{n}\Omega'(i_1,\ldots,i_k-1)\Omega'(i_{k+1}+1,\ldots,i_n).$$

Применим эту теорию к вероятностным задачам. Пусть $X_t,\ t \in \mathbb{Z}$ — независимые одинаково распеделенные случайные величины с непрерывной функцией распределения.

Теорема 4. *Пусть* $n \in \mathbb{N}$, $i_1, j_1, \ldots, i_n, j_n \in \mathbb{Z}_+$, $N := i_1 + \ldots + j_n$. *Тогда вероятность того, что при всех* $k = 1, \ldots, n$

$$X_{s''_{k-1}} < X_{s''_{k-1}+1} < \ldots < X_{s'_k} > X_{s'_k+1} > \ldots > X_{s''_k},$$

равна $\Omega'(i_1, j_1, \ldots, i_n, j_n)$.

Назовем $n \in \mathbb{Z}$ *точкой максимума* (*минимума*), если $X_n > X_{n-1}$, X_{n+1} ($X_n < X_{n-1}, X_{n+1}$). Точки максимума и минимума чередуются. Далее всюду предполагаем, что 0 — точка максимума. Пусть μ_0 — расстояние от 0 до следующей точки минимума, μ_1 — расстояние от этой точки минимума до следующей точки максимума, и т. д. Тогда (μ_t) — строго стационарная последовательность. Легко доказать, что для $k_0, \ldots, k_n \in \mathbb{N}$ выполняется равенство $\mathbf{P}\{\mu_0 = k_0, \ldots, \mu_n = k_n\} = 3\Omega'(1, k_0, \ldots, k_n, 1)$.

Например, $\mathbf{P}\{\mu_0 = k\} = 3(k^2 + 3k + 1)/(k + 3)!$, $\mathbf{E}\mu_0 = 3/2$, $Var\,\mu_0 = 6e - 63/4 \approx 0.560$, а $corr(\mu_0, \mu_1) = (2e^2 - 8e + 7)/(8e - 21) \approx 0.0427$.

Гипотеза. Имеет место закон больших чисел:

$$\frac{1}{n}\sum_{k=0}^{n-1} \mu_k \to \mathbf{E}\mu_0 = \frac{3}{2},\ n \to +\infty.$$

Для доказательства гипотезы достаточно доказать эргодичность последовательности (μ_t). На основании этого можно попытаться построить статистический тест на н.о.р. данного набора наблюдений $X_1, \ldots, X_n$.

Список литературы

1. Сачков В. Н. Введение в комбинаторные методы дискретной математики. — М.: Изд-во МЦНМО, 2004.

О КАНОНИЧЕСКИХ ПРЕДСТАВИТЕЛЯХ КЛАССОВ ПОДОБИЯ МАТРИЦ ВТОРОГО ПОРЯДКА НАД КОЛЬЦОМ ЦЕЛЫХ ЧИСЕЛ

С. В. Сидоров (Нижний Новгород)

В [1] исследовалась задача о подобии матриц второго порядка над кольцом целых чисел и, в частности, было доказано, что множество целочисленных матриц второго порядка, имеющих неприводимый над $\mathbf{Z}$ характеристический многочлен, разбивается на конечное число классов подобия над $\mathbf{Z}$. Интересным представляется изучить строение этих классов и найти канонические матрицы.

Если $\alpha \in \mathbf{Z}$, то для подобия матриц A и B необходимо и достаточно подобие матриц $A-\alpha E$ и $B-\alpha E$. Выбором α можно добиться того, что характеристический многочлен матрицы $A-\alpha E$ будет иметь вид λ^2-d или $\lambda^2-\lambda-d$. В работе изучаются классы подобия матриц, характеристический многочлен которых имеет вид λ^2-p^{2k+1}, где p – простое число.

Лемма 1. *Пусть матрица* $A=\begin{pmatrix} a & b \\ c & -a \end{pmatrix}$ *имеет характеристический многочлен* λ^2-p^{2k+1}, *где* p — *простое число,* $k \geq 0$.

1) *Если ни одно из чисел* a,b,c *не делится на* p, *то* A *подобна над* $\mathbf{Z}$ *матрице* $B=\begin{pmatrix} a' & b' \\ c' & -a' \end{pmatrix}$, *причем, если* $k \geq 1$, *то* a' *делится на* p, b' *делится на* p^2, c' *не делится на* p, *а если* $k=0$, *то* a', b' *делятся на* p, c' *не делится на* p.

2) *Если* a,c *делятся на* p, b *не делится на* p *и* $k \geq 0$, *то* A *подобна над* $\mathbf{Z}$ *матрице* $B=\begin{pmatrix} a' & b' \\ c' & -a' \end{pmatrix}$, *причем если* $k \geq 1$, *то* a' *делится на* p, b' *делится на* p^2, c' *не делится на* p, *а если* $k=0$, *то* a', b' *делятся на* p, c' *не делится на* p.

Лемма 2. *Пусть матрицы* $B'=\begin{pmatrix} pa' & p^2b' \\ c' & -pa' \end{pmatrix}$, $B''=\begin{pmatrix} pa'' & p^2b'' \\ c'' & -pa'' \end{pmatrix}$ *имеют характеристический многочлен* λ^2-p^{2k+1}, *где* p – *простое число и* c', c'' *не делятся на* p. *Пусть минимальное положительное решение уравнения Пелля* $x^2-py^2=\pm 1$ *не делится на* p. *Тогда матрицы* B', B'' *подобны только в том случае, когда подобны матрицы* $A'=\begin{pmatrix} a' & b' \\ c' & -a' \end{pmatrix}$, $A''=\begin{pmatrix} a'' & b'' \\ c'' & -a'' \end{pmatrix}$.

Обозначим через $N(d)$ число классов подобия матриц, имеющих характеристический многочлен $d(\lambda) = \lambda^2 - d$.

Теорема. *Если p — простое число, $N(p) = t$ и минимальное положительное решение уравнения Пелля $x^2 - py^2 = \pm 1$ не делится на p, то $N(p^{2k+1}) = (k+1)t$. Пусть $A_{1,j} = \begin{pmatrix} a_j & b_j \\ c_j & -a_j \end{pmatrix}, j = 1, \ldots, t$ — представители классов подобия для $k = 0$, причем можно считать, что c_j не делится на p. Тогда в качестве представителей $(k+1)t$ классов подобия можно взять матрицы $A_{k+1,it+j} = \begin{pmatrix} p^k a_j & p^{k+i} b_j \\ p^{k-i} c_j & -p^k a_j \end{pmatrix}, i = 0, \ldots, k; j = 1, \ldots, t$.*

Доказательство. Сначала докажем, что матрицы $A_{k+1,it+j}$ представляют различные классы подобия, т. е. не подобны при разных i и j. Индукция по k. При $k = 0$ утверждение превращается в одно из условий теоремы. Пусть доказано для $k-1$. То есть по предположению индукции матрицы $A_{k,it+j}$ с разными i и j не подобны. Отсюда следует, что матрицы $A_{k+1,it+j} = pA_{k,it+j}$, $i = 0, \ldots, k-1$ также не подобны. Далее, матрицы $A_{k,(k-1)t+j}$ не подобны при разных j по предположению индукции, значит, по лемме 2 матрицы $A_{k+1,kt+j}$ также не подобны при разных j. Осталось доказать, что матрицы $A_{k+1,it+j}$ с различными i не подобны. Это следует из того, что НОД элементов матрицы $A_{k+1,it+j}$ равен p^{k-i}НОД(a_j, b_j, c_j). При разных значениях i эти величины различны.

Теперь докажем, что любая матрица, имеющая характеристический многочлен $\lambda^2 - p^{2k+1}$, $k \geq 0$, подобна матрице $A_{k+1,it+j}$ для некоторых i и j. Снова применим индукцию по k. Случай $k = 0$ очевиден. Предположение индукции: каждая матрица, имеющая характеристический многочлен $\lambda^2 - p^{2k-1}$, подобна одной из матриц $A_{k,it+j} = \begin{pmatrix} p^{k-1} a_j & p^{k+i-1} b_j \\ p^{k-i-1} c_j & -p^{k-1} a_j \end{pmatrix}, i = 0, \ldots, k-1; j = 1, \ldots, t$.

Пусть $B = \begin{pmatrix} a & b \\ c & -a \end{pmatrix}$ — некоторая матрица, имеющая характеристический многочлен $\lambda^2 - p^{2k+1}$, т. е. $a^2 + bc = p^{2k+1}, k \geq 1$. Тогда возможны четыре случая:

I) $a \equiv 0 \pmod p$, $c \equiv 0 \pmod p$, $b \equiv 0 \pmod p$;

II) $a \equiv 0 \pmod p$, $c \not\equiv 0 \pmod p$, $b \equiv 0 \pmod{p^2}$;

III) $a \equiv 0 \pmod p$, $c \equiv 0 \pmod{p^2}$, $b \not\equiv 0 \pmod p$;

IV) $a \not\equiv 0 \pmod p$, $c \not\equiv 0 \pmod p$, $b \not\equiv 0 \pmod p$.

I. В первом случае $B = pB'$, причем матрица B' имеет характеристический многочлен $\lambda^2 - p^{2k-1}$. Следовательно, по пред-

положению индукции B' подобна некоторой матрице $A_{k,it+j} = \begin{pmatrix} p^{k-1}a_j & p^{k+i-1}b_j \\ p^{k-i-1}c_j & -p^{k-1}a_j \end{pmatrix}$. Но тогда B подобна матрице $A_{k+1,it+j} = pA_{k,it+j} = \begin{pmatrix} p^k a_j & p^{k+i}b_j \\ p^{k-i}c_j & -p^k a_j \end{pmatrix}$.

II. Во втором случае $B = \begin{pmatrix} pa' & p^2b' \\ c' & -pa' \end{pmatrix}$ и матрица $A' = \begin{pmatrix} a' & b' \\ c' & -a' \end{pmatrix}$ имеет характеристический многочлен $\lambda^2 - p^{2k-1}$. Значит, по предположению индукции A' подобна одной из матриц вида $A_{k,it+j}$. Так как $c' = c$ не делится на p, а матрицы $A_{k,it+j}$ при $i = 0, \ldots, k-2$ делятся на p, то A' подобна матрице вида $A_{k,(k-1)t+j} = \begin{pmatrix} p^{k-1}a_j & p^{2k-2}b_j \\ c_j & -p^{k-1}a_j \end{pmatrix}$ для некоторого j. Тогда по лемме 2 матрица B подобна матрице $A_{k+1,kt+j} = \begin{pmatrix} p^k a_j & p^{2k}b_j \\ c_j & -p^k a_j \end{pmatrix}$.

III. В третьем случае матрица B удовлетворяет пункту 2) леммы 1, поэтому B подобна матрице C, которая уже удовлетворяет второму случаю.

IV. В четвертом случае матрица B удовлетворяет пункту 1) леммы 1, поэтому B подобна матрице C, которая удовлетворяет второму случаю.

Следствие. *Если p — простое число, $N(p) = 1$ и минимальное положительное решение уравнения Пелля $x^2 - py^2 = \pm 1$ не делится на p, то $N(p^{2k+1}) = k+1$. В качестве представителей классов подобия можно взять матрицы $F_i = \begin{pmatrix} 0 & p^{2k-i+2} \\ p^{i-1} & 0 \end{pmatrix}$, $i = 1, \ldots, k+1$.*

Работа выполнена при финансовой поддержке РФФИ, проект 09-01-00545-а.

Список литературы

1. Шевченко В. Н., Сидоров С. В. О подобии матриц второго порядка над кольцом целых чисел // Известия вузов. Математика. — 2006. — № 4. — С. 57–64.

ОПРЕДЕЛИТЕЛЬ ГРАМА БАЗИСА ПРАВОГО МОДУЛЯ МНОГОИНДЕКСНОЙ ТРАНСПОРТНОЙ ЗАДАЧИ

Е. Б. Титова (Нижний Новгород)

Пусть $\mathbb{Q}$ — поле рациональных чисел, $\mathbb{Q}^N$ — линейное пространство столбцов с компонентами из $\mathbb{Q}$, а $\mathbb{Z}^N$ — столбцы из $\mathbb{Q}^N$ с целочисленными компонентами. Обозначим через $A \times B$ — кронекерово произведение матриц A и B; $e_1(n) = (1, 0, \ldots, 0)^\top$ — 1-й столбец единичной матрицы E_n порядка n; $\mathbf{1}^{m\times n}$ — матрицу размера $m \times n$, состоящую только из единиц. Для (M, N)-матрицы A с элементами из $\mathbb{Q}$ обозначим через $R_A = \{x \in \mathbb{Q}^N, Ax = 0\}$ правое нуль-пространство матрицы A, а через R — какой-нибудь его базис. Можно считать, что R — целочисленная $N \times (N - r)$-матрица, где r — ранг матрицы A. Множество $R_A^{\mathbb{Z}} = R_A \cap \mathbb{Z}^N$ назовем правым модулем матрицы A. Множество целочисленных линейных комбинаций столбцов матрицы R содержится в $R_A^{\mathbb{Z}}$, но, вообще говоря, с ним не совпадает. Это выполняется тогда и только тогда, когда матрица R унимодулярна (т. е. НОД базисных миноров равен 1). В этом случае R будем называть базисом правого модуля матрицы A.

Рассмотрим в качестве матрицы A матрицу ограничений s-арной k-индексной симметричной транспортной задачи $T = T_{s,k}(n_1, \ldots, n_k)$ (обозначения см., например, в [1]) с базисом правого модуля $R_{s,k}$. При $n_1 = n_2 = \ldots = n_k = n$ число ее строк $M = \binom{k}{s} n^{k-s}$, число столбцов $N = n^k$ и ранг $r_{s,k} = \sum_{i=s}^{k} \binom{k}{i} (n-1)^{k-i}$. Известно, что среди строк матрицы T найдется такая базисная система строк $T_{\mathcal{A}}$, $|\mathcal{A}| = r_{s,k}$, которая содержит базисный минор, равный 1. Очевидно, что $TR_{s,k} = 0 \Leftrightarrow T_{\mathcal{A}} R_{s,k} = 0$. Известно [1], что $|\det(R_{s,k}^\top R_{s,k})| = |\det(T_{\mathcal{A}} T_{\mathcal{A}}^\top)|$. Для оценки величины квадрата базисных миноров матрицы T вычислим определитель Грама $\det(R_{s,k}^\top R_{s,k})$.

Если $Q_n^* = \left[\dfrac{\mathbf{1}^{1\times(n-1)}}{-E_{n-1}}\right]$ — матрица $n \times (n-1)$ порядка, то обозначим $Q_n = [\mathbf{1}^{n\times 1} | Q_n^*]$, $\overline{Q}_n = [e_1(n) | Q_n^*]$.

Лексикографически упорядочим номера $J = \{j_1, j_2, \ldots, j_k\}$ ($j_\nu = 1, \ldots, n_\nu$ при $\nu = 1, \ldots, k$) векторов $\overline{q}_J = \overline{q}_{j_1}(n_1) \times \ldots \times \overline{q}_{j_k}(n_k)$ матрицы $\overline{Q} = \overline{Q}_{n_1} \times \ldots \times \overline{Q}_{n_k}$.

Теорема 1 [2]. *Базис $R_{s,k}(n_1, \ldots, n_k)$ правого модуля матрицы*

$T_{s,k}$ состоит из тех и только тех столбцов $\overline{q}_J$ матрицы $\overline{Q}$, для которых набор $J = \{j_1, j_2, \ldots, j_k\}$ содержит не более $(s-1)$ единиц.

Лемма 1. *Для произвольных k и $1 \le s \le k-1$ матрицу правого модуля можно представить в виде двух столбцовых блоков:*

$$R_{s,k}(n_1, \ldots, n_k) = [Q^*_{n_1} \times R_{s,k-1}(n_2, \ldots, n_k) | e_1(n_1) \times R_{s-1,k-1}(n_2, \ldots, n_k)],$$

где $R_{1,k}(n_1, \ldots, n_k) = Q^*_{n_1} \times \ldots \times Q^*_{n_k}$, $R(k, k, n_1, \ldots, n_k) = Q^*_{n_1 \cdot \ldots \cdot n_k}$.
Далее везде будем считать, что $n_1 = \ldots = n_k = n$.

Теорема 2. *Справедлива рекурсивная формула*

$$\det(R^\top_{s,k} R_{s,k}) = n^{\binom{k-1}{s-1}(n-1)^{k-s}} \det{}^{n-1}(R^\top_{s,k-1} R_{s,k-1}) \det(R^\top_{s-1,k-1} R_{s-1,k-1}).$$

Доказательство. Рассмотрим произведение матриц $R^\top_{s,k} R_{s,k} =$

$$= \left[\begin{array}{c|c} (Q^{*\top}_n Q^*_n) \times (R^\top_{s,k-1} R_{s,k-1}) & \mathbf{1}^{(n-1)\times 1} \times (R^\top_{s,k-1} R_{s-1,k-1}) \\ \hline \mathbf{1}^{1\times(n-1)} \times (R^\top_{s-1,k-1} R_{s,k-1}) & R^\top_{s-1,k-1} R_{s-1,k-1} \end{array} \right].$$

Так как $(Q^{*\top}_n Q^*_n) Q_{n-1} = Q_{n-1} D_{n-1}$, где $D_{n-1} = diag(n, 1, \ldots, 1)_{n-1}$, то введем трансформирующую матрицу

$$P = \left[\begin{array}{c|c} Q_{n-1} \times E_{rg_{s,k-1}} & \mathbf{0} \\ \hline \mathbf{0} & E_{rg_{s-1,k-1}} \end{array} \right],$$

где $rg_{s,k}$ — ранг матрицы $R_{s,k}$.

Поскольку $P^{-1} \cdot (R^\top_{s,k} R_{s,k}) \cdot P$ подобна матрице $R^\top_{s,k} R_{s,k}$, то

$$\det(R^\top_{s,k} R_{s,k}) = \det(P^{-1} \cdot (R^\top_{s,k} R_{s,k}) \cdot P) = \det{}^{n-2}(R^\top_{s,k-1} R_{s,k-1}) \times$$

$$\times \det \left[\begin{array}{c|c} n(R^\top_{s,k-1} R_{s,k-1}) & R^\top_{s,k-1} R_{s-1,k-1} \\ \hline (n-1)(R^\top_{s-1,k-1} R_{s,k-1}) & R^\top_{s-1,k-1} R_{s-1,k-1} \end{array} \right]. \qquad (1)$$

Далее заметим, что матрица

$$R_{s-1,k-1} = R_{s,k-1} \cdot \left[\begin{array}{c} E_{r_{s-1,k-1}} \\ \hline \mathbf{0}_{r_{s,k-1} - r_{s-1,k-1} \times r_{s-1,k-1}} \end{array} \right]$$

с точностью до перестановки столбцов. Отсюда видно, что каждый столбец из правого верхнего блока матрицы из правой части (1)

присутствует с коэффициентом n и в левом верхнем блоке этой матрицы, а каждый столбец из правого нижнего блока присутствует с коэффициентом $(n-1)$ и в левом нижнем блоке. Вычтем из каждого столбца правой полосы этой матрицы соответствующий столбец левой полосы с коэффициентом $1/n$. Тогда получим:

$$\det(R_{s,k}^{\top}R_{s,k}) = \det{}^{n-2}(R_{s,k-1}^{\top}R_{s,k-1})\times$$

$$\times \det\left[\begin{array}{c|c} n(R_{s,k-1}^{\top}R_{s,k-1}) & \mathbf{0} \\ \hline (n-1)(R_{s-1,k-1}^{\top}R_{s,k-1}) & \frac{1}{n}(R_{s-1,k-1}^{\top}R_{s-1,k-1}) \end{array}\right] =$$

$$= n^{rg_{s,k-1}-rg_{s-1,k-1}} \cdot \det{}^{n-1}(R_{s,k-1}^{\top}R_{s,k-1}) \cdot \det(R_{s-1,k-1}^{\top}R_{s-1,k-1}).$$

Так как $rg_{s,k} = n^k - r_{s,k} = n^k - \sum\limits_{i=0}^{k-s}\binom{k}{i}(n-1)^i$, то $rg_{s,k-1} - rg_{s-1,k-1} = \binom{k-1}{s-1}(n-1)^{k-s}$. Отсюда окончательно получаем утверждение теоремы.

Следствие 1. $\det(R_{s,k}^{\top}R_{s,k}) = n^{s\binom{k}{s}(n-1)^{k-s}}$.

Работа выполнена при финансовой поддержке гранта РФФИ 09-01-00545-а.

Список литературы

1. Шевченко В. Н. Многогранники многоиндексных транспортных задач: алгебраический подход // Материалы конференции "Дискретный анализ и исследование операций" (Новосибирск, 28 июня – 2 июля 2004 г.). — Новосибирск: Изд-во ин-та математики, 2004. — С. 64–70.

2. Титова Е. Б., Шевченко В. Н. Базис правого модуля матрицы ограничений многоиндексной транспортной задачи // Материалы конференции "Математика и кибернетика 2003" (Н. Новгород, 2003 г.). — С. 264–265.

КРАТЧАЙШИЕ МАРШРУТЫ И ПРЕРЫВАНИЯ В ЗАДАЧЕ OPEN SHOP С МАРШРУТИЗАЦИЕЙ МАШИН

И. Д. Черных (Новосибирск)

В классической задаче open shop заданы m машин и n работ, каждая работа J_j должна пройти обработку на каждой машине M_i, и

эта операция занимает p_{ji} единиц времени. Порядок выполнения операций каждой работы не фиксирован. Интервалы выполнения операций одной работы и одной машины не должны иметь общих внутренних точек. Требуется найти допустимое расписание, завершающее выполнение всех операций за кратчайшее время. Задача open shop разрешима за линейное время при $m = 2$ и является NP-трудной при $m \geqslant 3$ [1].

В классической постановке задачи open shop предполагается, что машина, завершив выполнение операции одной работы, может приступить к выполнению следующей операции без задержки. Мы рассматриваем один из возможных способов моделирования таких задержек: задачу с маршрутизацией машин.

Задача open shop с маршрутизацией была сформулирована в [2]. В этой постановке работы расположены в узлах транспортной сети, а машины, прежде чем выполнить операцию, должны доехать до соответствующего узла. Изначально все машины находятся в выделенной вершине, называемой *базой*, и должны туда вернуться после выполнения всех своих операций. Требуется построить допустимое расписание наименьшей возможной длины. Таким образом, задача open shop с маршрутизацией является обобщением двух NP-трудных задач: классической задачи open shop и метрической задачи коммивояжера (TSP). В [2] показана NP-трудность этой задачи уже для двух машин на двухвершинной сети, т. е. для случая, когда отдельные "подзадачи" open shop и TSP сложности не представляют.

Для этой "простой" задачи в [3] описан алгоритм с относительной оценкой точности 6/5. Для задачи с произвольной структурой транспортной сети в [2] предложен $\frac{7}{4}$-приближённый алгоритм для случая двух машин и $\frac{m+4}{2}$-приближённый алгоритм для задачи с m машинами. Новые алгоритмы с улучшенными оценками точности представлены в [4, 5]: для $m = 2$ описан алгоритм с оценкой $\frac{13}{8}$, для произвольного числа машин улучшена оценка точности алгоритма из [2] до $\frac{m+1}{2}$ (при $m \geqslant 3$) и описан алгоритм с относительной оценкой точности порядка $\sqrt{m}$. Для случая $m = 3$ в [4] описан алгоритм с оценкой точности $\frac{35}{18}$.

Задача open shop с маршрутизацией и разрешением прерываний частично исследована в случае двухвершинной сети: показана ее полиномиальная разрешимость в случае двух машин и NP-трудность в сильном смысле, если число машин является частью входа [6].

В данной работе мы ограничимся следующим случаем двухвершинной транспортной сети. Дано множество $\mathcal{M} = \{M_1, \ldots, M_m\}$ машин, два множества работ $\mathcal{J}^1$ и $\mathcal{J}^2$, первое множество работ

расположено в базе, а второе — в некотором узле, расположенном на расстоянии τ от базы, $\mathcal{J}^1 \cup \mathcal{J}^2 = \{J_1, \ldots, J_n\}$. Каждая машина $M_i \in \mathcal{M}$ должна выполнить операцию каждой работы $J_j \in \mathcal{J}^1 \cup \mathcal{J}^2$ за p_{ji} единиц времени. Для этого машина должна находиться в соответствующем узле, между которыми она передвигается с единичной скоростью. По окончании выполнения всех операций машина должна вернуться на базу. Требуется составить допустимое расписание, минимизирующее время возвращения на базу последней машины.

Обозначим за $l_{\max} = \max_i \sum_{j=1}^{n} p_{ij}$ — максимальную нагрузку машины, $d^k_{\max} = \max_{j \in \mathcal{J}^k} \sum_{i=1}^{m} p_{ij}$ — максимальную длину работы в узле $\mathcal{J}^k$, за $F_{\max}(S)$ — длину расписания S.

Для данного входа I рассмотрим четыре расписания: $S^*(I)$ — оптимальное расписание без прерываний, $S^{**}(I)$ — оптимальное расписание с разрешением прерываний, $S^*_1(I)$ и $S^{**}_1(I)$ — оптимальные расписания с одной поездкой каждой машины во второй узел без прерываний и с разрешением прерываний соответственно. Очевидны следующие неравенства (для однородности используем обозначения $\nu_i(I)$):

$$\nu_1(I) \doteq F_{\max}(S^{**}(I)) \leqslant \nu_2(I) \doteq F_{\max}(S^{**}_1(I)) \leqslant F_{\max}(S^*_1(I)),$$

$$F_{\max}(S^{**}(I)) \leqslant \nu_3(I) \doteq F_{\max}(S^*(I)) \leqslant \nu_4(I) \doteq F_{\max}(S^*_1(I)).$$

Кроме того, справедлива следующая нижняя оценка оптимума каждой из этих постановок:

$$F_{\max}(S^{**}(I)) \geqslant \nu_0(I) \doteq \max\{l_{\max} + 2\tau, d^1_{\max}, d^2_{\max} + 2\tau\}.$$

Нас интересует вопрос, насколько могут отличаться друг от друга участники этих неравенств при фиксированном числе машин. Для ответа на этот вопрос обозначим через $\mathcal{I}_m$ множество m-машинных входов рассматриваемой задачи, для которых $\nu_0(I) > 0$, и рассмотрим функции

$$\delta^i_j(m) \doteq \sup_{I \in \mathcal{I}_m} \frac{\nu_i(I)}{\nu_j(I)}, 0 \leqslant j < i \leqslant 4 \text{ кроме случая } (i = 3)\&(j = 2).$$

Найденные на данный момент значения этих функций приводятся в следующей таблице:

m	δ^1_0	δ^2_0	δ^3_0	δ^4_0	δ^2_1	δ^3_1	δ^4_1	δ^4_2	δ^4_3
2	1	1	6/5	5/4	1	6/5	5/4	5/4	5/4
3	$[\frac{8}{7}, \frac{5}{3}]$	$[\frac{7}{6}, \frac{5}{3}]$	$[\frac{4}{3}, \frac{49}{25}]$	$[\frac{4}{3}, \frac{73}{36}]$	$[\frac{7}{6}, \frac{5}{3}]$	$[\frac{4}{3}, \frac{49}{25}]$	$[\frac{4}{3}, \frac{73}{36}]$	$[\frac{4}{3}, \frac{73}{36}]$	$[\frac{4}{3}, \frac{73}{36}]$
∞	$\leqslant 2$	$\leqslant 2$	$\leqslant 3.5$	$\leqslant 3.5$	$\leqslant 2$	$\leqslant 3.5$	$\leqslant 3.5$	$\leqslant 3.5$	$\leqslant 3.5$

Нижние оценки величин в этой таблице обеспечиваются подходящими примерами задачи, а верхние — приближенными алгоритмами с соответствующими оценками точности.

Работа выполнена при финансовой поддержке РФФИ, проект 08-01-00370.

Список литературы

1. Gonzalez T., Sahni S. Open shop scheduling to minimize finish time // J. ACM 1976. — V. 23, № 4. — P. 665–679.

2. Averbakh I., Berman O., Chernykh I. The routing open-shop problem on a network: complexity and approximation // European Journal of Operational Research. — 2006. — V. 173, № 2. — P. 531–539.

3. Averbakh I., Berman O., Chernykh I. A $\frac{6}{5}$-approximation algorithm for the two-machine routing open-shop problem on a 2-node network. // European Journal of Operational Research. — 2005. — V. 166, № 1. — P. 3–24.

4. Дрюк Н. С., Кононов А. В., Севастьянов С. В., Черных И. Д. Эффективные алгоритмы приближённого решения задачи open shop с маршрутизацией машин // Рабочая статья.

5. Chernykh I., Kononov A., Sevastyanov S. Efficient approximation algorithms for the routing open-shop problem // Submitted to Computers and Operations Research.

6. Пяткин А. В., Черных И. Д.. Задача открытого типа с маршрутизацией и разрешением прерываний на двухвершинной сети // Материалы IV Всероссийской конференции "Проблемы оптимизации и экономический приложения" (Омск, 29 июня – 4 июля 2009). — С. 158.

ОБ f-ВЕКТОРАХ РЕГУЛЯРНЫХ ТРИАНГУЛЯЦИЙ ТОЧЕЧНЫХ КОНФИГУРАЦИЙ

В. Н. Шевченко, Д. В. Груздев (Нижний Новгород)

Получен ряд необходимых соотношений для того, чтобы целочисленный вектор являлся f-вектором регулярной триангуляции точечной конфигурации, и выдвинута гипотеза о достаточности данных условий.

Рассмотрим d-мерный выпуклый многогранник $M \subset \mathrm{R}^d$, который будем называть также *d-мерным политопом*, и обозначим через $\Gamma_i(M)$ множество его i-мерных граней, $i = -1, \ldots, d$. При этом $\Gamma_{-1}(M) = \{\emptyset\}$ и $\Gamma_d(M) = \{M\}$. Если $|\Gamma_0(M)| = d + 1$, то политоп M называется *d-мерным симплексом*.

Выпуклую оболочку множества точек A' обозначим через $[A']$. Конечное множество точек $A = \{a_1, \ldots, a_n\} \subset \mathrm{R}^d$, выпуклая оболочка $[A]$ которого есть d-мерный политоп, называется *d-мерной точечной конфигурацией*. Множество *d-мерных* точечных конфигураций обозначим через $\mathcal{A}_d$.

Триангуляцией d-мерной точечной конфигурации A называется такое множество $T = \{S_1, \ldots, S_t\}$ d-мерных симплексов $S_1, \ldots, S_t$ с вершинами из A, что их объединение есть политоп $[A]$ и пересечение любых двух симплексов из T является их общей гранью (возможно, пустой). Положим $\Gamma_i(T) = \bigcup_{j=1}^{t} \Gamma_i(S_j)$ и $f_i^T = |\Gamma_i(T)|$ при $i = -1, \ldots, d$ и заметим, что $\Gamma_{-1}(T) = \{\emptyset\}$ и $f_{-1}^T = 1$. Вектор $f^T = (f_0^T, f_1^T, \ldots, f_d^T)$ называется *f-вектором* триангуляции T, а полином $f^T(\lambda) = \sum_{i=-1}^{d} f_i^T \lambda^{i+1}$ называется *f-полиномом* триангуляции T. Множество триангуляций точечной конфигурации A обозначим через $\mathcal{T}(A)$.

Из [1] следует, что для триангуляци T d-мерной точечной конфигурации существуют, единственны и являются неотрицательными целые числа $\gamma_0^T, \ldots, \gamma_{d+1}^T$ такие, что $f^T(\lambda) = \sum_{i=0}^{d+1} \gamma_i^T \lambda^i (1+\lambda)^{d+1-i}$, причём $\gamma_0^T = 1$ и $\gamma_{d+1}^T = 0$. Положим $\gamma_i^T = 0$ при целых $i \geq d+2$. Вектор $\gamma^T = (\gamma_0^T, \gamma_1^T, \ldots)$ называется *γ-вектором* триангуляции T.

Рассмотрим $A = \{a_1, \ldots, a_n\} \in \mathcal{A}_d$ и такие $\lambda_1, \ldots, \lambda_n \in \mathrm{R}$, что $A' = \{a_1', \ldots, a_n'\} \in \mathcal{A}_{d+1}$, где $a_i' = (a_i, \lambda_i)$, $i = 1, \ldots, n$. Теперь рассмотрим множество T'^+ тех d-мерных граней политопа $[A']$, внутренняя нормаль к которым имеет положительную последнюю компоненту. Если все такие грани являются симплексами, то $T^+ = \{[a_{i_1}, \ldots, a_{i_{d+1}}] \,:\, [a_{i_1}', \ldots, a_{i_{d+1}}'] \in T'^+\}$ является триангуляцией из $\mathcal{T}(A)$, называемой *регулярной* (regular, правильной, см., например, [2]). Если $A \in \mathcal{A}_d$ и $|A| = d+1$, то единственная триангуляция из $\mathcal{T}(A) = \{\{[A]\}\}$ также называется *регулярной* [2].

Через $\mathcal{T}_d^R$ обозначим множество регулярных триангуляций d-мерных точечных конфигураций, а через H_d^R обозначим множество γ-векторов регулярных триангуляций из $\mathcal{T}_d^R$.

Теперь приведём определение так называемой i-ой *псевдостепени* числа b [3], которое будет использовано для формулировки основного утверждения. Известно, что для натуральных чисел b и i существует единственное биномиальное представление $b = \binom{b_i}{i} + \binom{b_{i-1}}{i-1} + \cdots + \binom{b_j}{j}$, где $b_i > b_{i-1} > \cdots > b_j \geq j \geq 1$. Тогда число

$b^{<i>} = \binom{b_i+1}{i+1} + \binom{b_{i-1}+1}{i} + \cdots + \binom{b_j+1}{j+1}$ называется *i-ой псевдостепенью* числа b. Также положим $0^{<i>} = 0$.

Теорема 1. *Для того, чтобы целочисленный вектор* $\gamma = (\gamma_0, \gamma_1, \dots)$ *принадлежал* H_d^R, *необходимо, чтобы выполнялись следующие условия:*

1) $\gamma_0 = 1$, $\gamma_i \geq 0$ *при* $i = 1, \dots, d$ *и* $\gamma_k = 0$ *при целых* $k \geq d+1$,

2) $\gamma_{\lfloor \frac{d+1}{2} \rfloor} \geq \gamma_{\lfloor \frac{d+1}{2} \rfloor + 1} \geq \cdots \geq \gamma_d$ *и* $\gamma_i - \gamma_{d+1-i} \geq 0$ *при* $i = 1, \dots, \lfloor \frac{d-1}{2} \rfloor$,

3) $\gamma_{i+1} - \gamma_{j-i} \leq (\gamma_i - \gamma_{j+1-i})^{<i>}$ *при* $j = d, \dots, 2d$ *и* $i = 1, \dots, \lfloor \frac{j}{2} \rfloor - 1$.

Заметим, что условие 3 теоремы 1 при $j = 2d$ является известным [4] необходимым условием $\gamma_{i+1} \leq (\gamma_i)^{<i>}$, $i = 1, \dots, d-1$, для того, чтобы неотрицательный целочисленный вектор $\gamma = (\gamma_0, \gamma_1, \dots)$ являлся γ-вектором триангуляции d-мерной точечной конфигурации.

Гипотеза. *Условия* 1–3 *теоремы* 1 *являются не только необходимыми, но и достаточными для того, чтобы целочисленный вектор* $\gamma = (\gamma_0, \gamma_1, \dots)$ *принадлежал* H_d^R.

Обозначив через Z_+ множество целых неотрицательных чисел и положив $H'_d = \{(\gamma_0, \gamma_1, \dots) \in \{1\} \times \mathrm{Z}_+^d \times \{0\}^\infty : \gamma_k - \gamma_{j+1-k} \geq 0,\ \gamma_{i+1} - \gamma_{j-i} \leq (\gamma_i - \gamma_{j+1-i})^{<i>},\ j = d, \dots, 2d,\ k = 1, \dots, \lfloor \frac{j}{2} \rfloor,\ i = 1, \dots, \lfloor \frac{j}{2} \rfloor - 1\}$, заметим, что утверждение теоремы 1 эквивалентно включению $H_d^R \subseteq H'_d$, а гипотеза 1 может быть представлена в виде равенства $H_d^R = H'_d$. В заключение, положив $H_d^0 = \{1\} \times \mathrm{Z}_+^{\lfloor \frac{d}{2} \rfloor} \times \{0\}^\infty$, заметим, что из [3] следует, что $H_d^R \cap H_d^0 = H'_d \cap H_d^0$.

Работа выполнена при поддержке РФФИ, проект 09-01-00545-а.

Список литературы

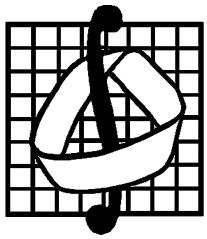
1. Kleinschmidt P., Smilansky Z. New results for simplicial spherical polytopes // Discrete and Computation Geometry. DIMACS Series in Discrete Mathematics and Theoretical Computer Science. — 1991. — V. 6. — P. 187–197.

2. Lee C. W. Regular triangulations of convex polytopes // DIMACS Series in Discrete Mathematics and Theoretical Computer Science. 1991. — V. 4. — P. 443–456.

3. Billera L. J., Lee C. W. A proof of the sufficiency of McMullen's conditions for f-vectors of simplicial convex polytopes. // Journal of combinatorial theory. Ser A. — 1981. — V. 31. — P. 237–255.

4. Macaulay F. S. Some properties of enumeration in the theory of modular systems // Proceedings of the London Mathematical Society. — 1927. — V. 26. — P. 531–555.

МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
имени М. В. ЛОМОНОСОВА



МЕХАНИКО-МАТЕМАТИЧЕСКИЙ ФАКУЛЬТЕТ

МАТЕРИАЛЫ

X Международного семинара

«ДИСКРЕТНАЯ МАТЕМАТИКА И ЕЕ ПРИЛОЖЕНИЯ»

(Москва, 1–6 февраля 2010 г.)

Издательство механико-математического факультета МГУ

Москва 2010

М34
УДК 519.7

Издание осуществлено при поддержке Российского фонда фундаментальных исследований по проекту 10–01–06004–г

М34 Материалы X Международного семинара «Дискретная математика и ее приложения»(Москва, МГУ, 1–6 февраля 2010 г.) / Под редакцией О. М. Касим-Заде. — М.: Изд-во механико-математического факультета МГУ, 2010. — 549 с.

Сборник содержит материалы X Международного семинара «Дискретная математика и ее приложения», проходившего на механико-математическом факультете МГУ имени М. В. Ломоносова с 1 по 6 февраля 2010 г. при поддержке Российского фонда фундаментальных исследований (проект 10–01–06004). Для студентов, аспирантов и научных работников в области дискретной математики и математической кибернетики.

Научное издание

МАТЕРИАЛЫ
X МЕЖДУНАРОДНОГО СЕМИНАРА
«ДИСКРЕТНАЯ МАТЕМАТИКА И ЕЕ ПРИЛОЖЕНИЯ»
(Москва, МГУ, 1–6 февраля 2010 г.)

Под общей редакцией О. М. КАСИМ-ЗАДЕ

Редакционная группа:
К. А. Зыков, Р. М. Колпаков, В. В. Кочергин, А. В. Чашкин

Ответственный за выпуск *В. В. Кочергин*

Н/К
ИД № 04059 от 20.02.2001 Подписано к печати 10.03.2010. Формат 60 × 90/16.
Бумага типогр. № 1. Печ. л. 34,5. Тираж 300 экз.
Издательство механико-математического факультета МГУ. 119991, Москва, Ленинские горы, МГУ.
Отпечатано с оригинал-макета в типографии ООО «Гипрософт», Москва

© Коллектив авторов, 2010

ПРЕДИСЛОВИЕ

X Международный семинар «Дискретная математика и ее приложения» проходил на механико-математическом факультете МГУ имени М. В. Ломоносова с 1 по 6 февраля 2010 г. при поддержке Российского фонда фундаментальных исследований (проект 10–01–06004–г).

Оргкомитетом семинара до начала его работы были разосланы информационные письма в ведущие научные центры и университеты стран СНГ, отобраны наиболее интересные доклады и сообщения для заслушивания на пленарных и секционных заседаниях.

Семинар собрал более 250 участников (в том числе более 60 докторов наук) из 40 научных центров России, Беларуси, Украины, Молдовы и Азербайджана.

Работа семинара проходила в шести секциях:

— синтез, сложность и надежность управляющих систем,

— теория функциональных систем,

— комбинаторный анализ и теория графов,
подсекции:
  — комбинаторный анализ,
  — теория графов,

— математическая теория интеллектуальных систем,

— дискретная геометрия,

— теория кодирования и математические воросы теории защиты информации

Всего было заслушано 18 пленарных и 194 секционных доклада; содержание большинства из них отражено в настоящем сборнике.

Тексты публикуются в авторской редакции (исправлены замеченные опечатки).

Подсекция «Теория графов»

О 2-СВЯЗНОСТИ ПОДМНОЖЕСТВ В СЛОЯХ n-МЕРНОЙ k-ЗНАЧНОЙ РЕШЕТКИ

Т. В. Андреева (Москва)

В решении проблемы Дедекинда (см., например, [1]) важную роль играют 2-связные множества в единичном кубе. В сообщении доказывается 2-связность лексикографических отрезков в k-значной решетке для $k \geq 2$.

Пусть на множестве $E_k = \{0, 1, \ldots, k-1\}$ задано отношение порядка "$<$", при котором $0 < 1 < \ldots < k-1$. Для сокращения записи в дальнейшем индекс k будем опускать.

Множество $E^n = \{\tilde{a} = (a_1, \ldots, a_n) : a_r \in E, r = 1, \ldots, n\}$ с отношением частичного порядка "$\leq$" называется *n-мерной k-значной решеткой*.

Величина $\|\tilde{a}\| = \sum_{r=1}^{n} a_r$ называется *весом вершины* $\tilde{a} \in E^n$. Множество $E_i^n = \left\{\tilde{a} \in E^n : \|\tilde{a}\| = i\right\}$ будем называть *i-м слоем* E^n.

Если задан набор $\tilde{\sigma} = (\sigma_1, \ldots, \sigma_p)$, то *гранью* E^n назовем множество $E_{\tilde{\sigma}}^n = \{\tilde{a} \in E^n : a_r = \sigma_r,\ r = 1, \ldots, p\}$.

Будем рассматривать *лексикографический порядок* "$\prec$" на множестве E^n, при котором $\tilde{a} = (a_1, \ldots, a_n) \prec \tilde{b} = (b_1, \ldots, b_n)$, если либо $a_1 < b_1$, либо $a_1 = b_1, \ldots, a_{t-1} = b_{t-1}$, $a_t < b_t$ для некоторого $t \geq 2$.

Множество A, состоящее из идущих подряд в лексикографическом порядке $|A|$ вершин слоя E_i^n, называется *лексикографическим отрезком* в E_i^n, сокращенно ЛО.

Лексикографический отрезок A называется *левым* (*правым*) в E_i^n, если он состоит из первых (соответственно, последних) вершин слоя E_i^n. Сокращенно будем называть его ЛЛО (ПЛО).

Множество $\partial A = \{\tilde{u} \in E_{i-1}^n : \exists \tilde{a} \in A, \tilde{u} \leq \tilde{a}\}$ называется *границей множества* $A \subseteq E_i^n$. Положим $\partial \tilde{a} = \partial\{\tilde{a}\}$.

Рассмотрим граф $G_A = (A, E_G)$, в котором $\{\tilde{a}, \tilde{b}\} \in E_G$ тогда и только тогда, когда $\partial\tilde{a} \cap \partial\tilde{b} \neq \emptyset$. Множество A называется *2-связным*, если граф G_A является связным (см., например, [2]).

Расстоянием между вершинами $\tilde{a} = (a_1, \ldots, a_n)$ и $\tilde{b} = (b_1, \ldots, b_n)$ называется величина $\rho(\tilde{a}, \tilde{b}) = \sum_{r=1}^{n} |a_r - b_r|$.

Заметим, что $\partial\tilde{a} \cap \partial\tilde{b} \neq \emptyset$ для $\tilde{a}, \tilde{b} \in E_i^n$ тогда и только тогда, когда $\rho(\tilde{a}, \tilde{b}) = 2$.

Теорема 1. *Всякий ЛЛО в E_i^n является 2-связным.*

Доказательство. ЛЛО мощности m в E_i^n обозначим $L_i(m)$.

Индукция по m. Множество $L_i(1)$ является 2-связным по определению. Предположим, что $L_i(m)$ является 2-связным при $m \geq 1$.

Рассмотрим $L_i(m+1)$ и положим $\tilde{a} = L_i(m+1) \setminus L_i(m)$. В силу предположения индукции достаточно показать, что найдется вершина $\tilde{b} \in L_i(m)$ такая, что $\rho(\tilde{a}, \tilde{b}) = 2$. Очевидно, что $\tilde{b} \in L_i(m)$ тогда и только тогда, когда $\tilde{b} \prec \tilde{a}$.

Рассмотрим некоторую вершину $\tilde{c} \in L_i(m)$. Поскольку $\tilde{c} \prec \tilde{a}$, для некоторого $t \geq 1$ имеет место $c_r = a_r$ при $r < t$ и $c_t < a_t$. Кроме того, найдется $j > t$, для которого $c_j > a_j$, в противном случае вершины $\tilde{a}$ и $\tilde{c}$ лежали бы в разных слоях E^n. Следовательно, для некоторых t, j таких, что $1 \leq t < j \leq n$, выполнено $a_t > 0$, $a_j < k - 1$.

Положим $\tilde{b} = (a_1, \ldots, a_{t-1}, a_t - 1, a_{t+1} \ldots, a_{j-1}, a_j + 1, a_{j+1}, \ldots, a_n)$. Очевидно, что $\tilde{b} \prec \tilde{a}$ и $\rho(\tilde{a}, \tilde{b}) = 2$, следовательно, множество $L_i(m+1)$ является 2-связным. Теорема доказана.

Теорема 2. *Всякий ПЛО в E_i^n является 2-связным.*

Доказательство аналогично доказательству теоремы 1.

Следствие 1. *Множество $E_i^n \cap E_{\tilde{\sigma}}^n$ является 2-связным.*

Доказательство. Положим $A = E_i^n \cap E_{\tilde{\sigma}}^n$. Множество A изоморфно слою E_{i-s}^{n-p} в решетке E^{n-p}. Поскольку слой решетки является ЛЛО, по теореме 1 он 2-связен. Следовательно, множество A является 2-связным в E^n.

Следствие 2. *Множество A, состоящее из первых $|A|$ в лексикографическом порядке вершин множества $E_i^n \cap E_{\tilde{\sigma}}^n$, является 2-связным.*

Следствие 3. *Множество A, состоящее из последних $|A|$ в лексикографическом порядке вершин множества $E_i^n \cap E_{\tilde{\sigma}}^n$, является 2-связным.*

Теорема 3. *Пусть наборы $\tilde{\sigma}^1, \ldots, \tilde{\sigma}^m$ таковы, что $\tilde{\sigma}^1 \prec \ldots \prec \tilde{\sigma}^m$, множество $E_i^n \cap E_{\tilde{\sigma}^r}^n$ не пусто при $r = 1, \ldots, m$, а также для каждого номера l найдется номер $r < l$ такой, что выполнено либо*

(1) $\rho(\tilde{\sigma}^r, \tilde{\sigma}^l) = 1$, *либо*

(2) $\rho(\tilde{\sigma}^r, \tilde{\sigma}^l) = 2$ *и* $\|\tilde{\sigma}^r\| = \|\tilde{\sigma}^l\|$.

Тогда множество $\left(E_{\tilde{\sigma}^1}^n \cup \ldots \cup E_{\tilde{\sigma}^m}^n\right) \cap E_i^n$ *является 2-связным.*

Доказательство. Положим $A_r = E_i^n \cap E_{\tilde{\sigma}^r}^n$, $r = 1, \ldots, m$. Тогда $\big(E_{\tilde{\sigma}^1}^n \cup \ldots \cup E_{\tilde{\sigma}^m}^n\big) \cap E_i^n = A_1 \cup \ldots \cup A_m$.

Заметим, что множества $A_1, \ldots, A_m$ попарно не пересекаются, и, в силу следствия 1, каждое из множеств A_r является 2-связным.

Индукция по m. При $m = 1$ множество A_1 является 2-связным. Предположим, что при $m \geq 1$ множество $A_1 \cup \ldots \cup A_m$ является 2-связным.

Рассмотрим множество $A = A_1 \cup \ldots \cup A_{m+1}$. В силу предположения индукции достаточно показать, что для некоторой вершины $\tilde{a} \in A_{m+1}$ найдется вершина $\tilde{b} \in A \setminus A_{m+1}$ такая, что $\rho(\tilde{a}, \tilde{b}) = 2$.

Пусть $\tilde{a} = (\sigma_1^{m+1}, \ldots, \sigma_p^{m+1}, a_{p+1}, \ldots, a_n)$. По условию теоремы найдется номер $r \leq m$ такой, что для $\tilde{\sigma}^r$ и $\tilde{\sigma}^{m+1}$ выполнено либо (1), либо (2).

Если выполнено (1), то $\|\tilde{\sigma}^r\| = \|\tilde{\sigma}^{m+1}\| - 1$. Если $a_{p+1} = \ldots = a_n = k - 1$, то $\|\tilde{b}\| < \|\tilde{a}\|$ для любого $\tilde{b} \in A_r$, это противоречит тому, что $\|\tilde{a}\| = \|\tilde{b}\| = i$. Значит, $a_q \leq k-2$ для некоторого $q \geq p+1$. Положим $\tilde{b} = (\sigma_1^r, \ldots, \sigma_p^r, a_{p+1}, \ldots, a_{q-1}, a_q + 1, a_{q+1}, \ldots, a_n)$. Заметим, что $\tilde{b} \in A_r$, поскольку $A_r = E_i^n \cap E_{\tilde{\sigma}^r}^n$. Из (1) и определения вершины $\tilde{b}$ следует, что

$$\rho(\tilde{a}, \tilde{b}) = \rho(\tilde{\sigma}^r, \tilde{\sigma}^{m+1}) + \rho\big((a_{p+1}, \ldots, a_n), (a_{p+1}, \ldots, a_q + 1, \ldots, a_n)\big) = 2.$$

Если выполнено (2), положим $\tilde{b} = (\sigma_1^r, \ldots, \sigma_p^r, a_{p+1}, \ldots, a_n)$. Заметим, что $\tilde{b} \in A_r$, поскольку $A_r = E_i^n \cap E_{\tilde{\sigma}^r}^n$. Из (2) и определения вершины $\tilde{b}$ следует, что $\rho(\tilde{a}, \tilde{b}) = 2$. Теорема доказана.

Замечание. Из теоремы 3 следует, что не всякий ЛО является 2-связным.

При $k = 2$ рассмотрим множество $(E_{2;(0,1,1)}^n \cup E_{2;(1,0,0)}^n) \cap E_{2,i}^n$. Оно является ЛО, но $\rho\big((0,1,1),(1,0,0)\big) = 3 > 2$.

Если же $k > 2$, рассмотрим множество $(E_{k;(0,k-1)}^n \cup E_{k;(1,0)}^n) \cap E_{k,i}^n$. Оно является является ЛО, но $\rho\big((0,k-1),(1,0)\big) = k > 2$.

Работа выполнена при поддержке РФФИ, проект 10-01-00768.

Список литературы

1. Сапоженко А. А. Проблема Дедекинда и метод граничных функционалов // Математические вопросы кибернетики. Вып. 9. — М.: Наука, 2000. — С. 161–220.

2. Сапоженко А. А. О числе связных подмножеств с заданной мощностью границы в двудольных графах // Методы дискретного

анализа в решении комбинаторных задач. Вып. 45. — Новосибирск, 1987. — С. 42–70.

ТРЕХИНДЕКСНЫЕ ТРАНСПОРТНЫЕ ЗАДАЧИ С ВЛОЖЕННОЙ СТРУКТУРОЙ

Л. Г. Афраймович, М. Х. Прилуцкий (Нижний Новгород)

Существует широкий класс прикладных задач распределения ресурсов, формализуемых в виде многоиндексных задач линейного программирования транспортного типа. Примерами таких задач являются [1–4] транспортная задача с промежуточными пунктами, задача объемно-календарного планирования для подразделений предприятия, задача распределения мощностей каналов передачи данных провайдерами сети Интернет, задача формирования портфеля заказов и др. Одним из перспективных направлений при разработке эффективных алгоритмов исследования многоиндексных транспортных задач линейного программирования является нахождение подклассов задач, для решения которых применимы потоковые методы.

Для описания многоиндексных задач воспользуемся следующей формализацией. Пусть заданно множество индексов $N(s) = \{i_1, i_2, \ldots, i_s\}$ и множество $M \subseteq 2^{N(s)}$. Тогда через $W(M)$ будем обозначать многоиндексную задачу линейного программирования транспортного типа с множеством индексов $N(s)$ и системой ограничений, состоящей, для каждого $f \in M$, из ограничений на подсуммы, в которых суммирование происходит по всем индексам множества f при фиксированных наборах значений индексов из $N(s)\setminus f$. Не уменьшая общности будем предполагать, что каждый индекс принимает не менее двух различных значений. Через $D(M)$ обозначим матрицу системы ограничений задачи $W(M)$.

В общем случае для решения задачи $W(M)$ могут быть использованы лишь универсальные методы решения задач линейного программирования. Специфика поставленной задачи (линейные ограничения транспортного типа) позволила для частного класса рассматриваемых задач предложить более эффективные алгоритмы их решения, основанные на сводимости к потоковым алгоритмам [1]. В рамках данной работы будем применять концепцию сводимости задач линейного программирования к задаче поиска потока минимальной стоимости, введенную в работах [1, 2].

Определение. *Множество* M, $M \subseteq 2^{N(s)}$, *называется* k*-вложенным, если существует разбиение множества* M *на* k *подмножеств* $M_i = \{f_1^{(i)}, f_2^{(i)}, \ldots, f_{m_i}^{(i)}\}$, $i = \overline{1,k}$, *такое, что* $f_j^{(i)} \subseteq f_{j+1}^{(i)}$, $j = \overline{1, m_i - 1}$, $i = \overline{1,k}$.

Теорема 1. *Для того, чтобы задача* $W(M)$ *сводилась к задаче поиска потока минимальной стоимости достаточно, чтобы множество* M *было* 2*-вложенным.*

Теорема 2. *Для того, чтобы задача* $W(M)$ *сводилась к задаче поиска потока минимальной стоимости необходимо, чтобы матрица* $D(M)$ *была абсолютно унимодулярной.*

Утверждение 1. *Если задача* $W(M)$ *сводится к задаче поиска потока минимальной стоимости, то также сводится любая задача* $W(M')$, *где* $M' \subseteq M$.

Утверждение 2. *Если задача* $W(M)$ *не сводится к задаче поиска потока минимальной стоимости, то также не сводится любая задача* $W(M')$, *где* $M \subset M'$.

Двухиндексный случай является наиболее исследованным. Более того, при $s = 2$ любое множество M будет являться 2-вложенным.

Далее пусть $s = 3$ и $N(s) = \{i_1, i_2, i_3\}$. Всего существует $2^{2^s} = 256$ различных множеств M, определяющих, соответственно, 256 различных "типов" задач $W(M)$. Максимальными по мощности 2-вложенными множествами здесь будут являться

- $M_1^+ = \{\{i_1, i_2, i_3\}, \{i_1, i_2\}, \{i_1, i_3\}, \{i_1\}, \{i_2\}, \emptyset\}$;
- $M_2^+ = \{\{i_1, i_2, i_3\}, \{i_1, i_2\}, \{i_1, i_3\}, \{i_1\}, \{i_3\}, \emptyset\}$;
- $M_3^+ = \{\{i_1, i_2, i_3\}, \{i_1, i_2\}, \{i_1, i_3\}, \{i_2\}, \{i_3\}, \emptyset\}$;
- $M_4^+ = \{\{i_1, i_2, i_3\}, \{i_1, i_2\}, \{i_2, i_3\}, \{i_1\}, \{i_2\}, \emptyset\}$;
- $M_5^+ = \{\{i_1, i_2, i_3\}, \{i_1, i_2\}, \{i_2, i_3\}, \{i_1\}, \{i_3\}, \emptyset\}$;
- $M_6^+ = \{\{i_1, i_2, i_3\}, \{i_1, i_2\}, \{i_2, i_3\}, \{i_2\}, \{i_3\}, \emptyset\}$;
- $M_7^+ = \{\{i_1, i_2, i_3\}, \{i_1, i_3\}, \{i_2, i_3\}, \{i_1\}, \{i_2\}, \emptyset\}$;
- $M_8^+ = \{\{i_1, i_2, i_3\}, \{i_1, i_3\}, \{i_2, i_3\}, \{i_1\}, \{i_3\}, \emptyset\}$;
- $M_9^+ = \{\{i_1, i_2, i_3\}, \{i_1, i_3\}, \{i_2, i_3\}, \{i_2\}, \{i_3\}, \emptyset\}$.

Было найденно, что матрицы систем ограничений, определяемые следующими множествами, не являются абсолютно унимодулярными:

- $M_1^- = \{\{i_1, i_2\}, \{i_1, i_3\}, \{i_2, i_3\}\}$;
- $M_2^- = \{\{i_1, i_2, i_3\}, \{i_1\}, \{i_2\}, \{i_3\}\}$;
- $M_3^- = \{\{i_1, i_2\}, \{i_1\}, \{i_2\}, \{i_3\}\}$;
- $M_4^- = \{\{i_1, i_3\}, \{i_1\}, \{i_2\}, \{i_3\}\}$;
- $M_5^- = \{\{i_2, i_3\}, \{i_1\}, \{i_2\}, \{i_3\}\}$.

Таким образом, среди трехиндексных задач открытым остается вопрос сводимости для задач, определяемых следующими множествами

- $M_1 = \{\{i_1\}, \{i_2\}, \{i_3\}\}$;
- $M_2 = \{\{i_1\}, \{i_2\}, \{i_3\}, \emptyset\}$.

Список литературы

1. Афраймович Л. Г., Прилуцкий М. Х. Многоиндексные задачи распределения ресурсов в иерархических системах // Автоматика и телемеханика. — 2006. — № 6. — С. 194–205.

2. Афраймович Л. Г., Прилуцкий М. Х. Многопродуктовые потоки в древовидных сетях // Известия РАН. Теория и системы управления. — 2008. — № 2. — С. 57–63.

3. Прилуцкий М. Х. Многокритериальные многоиндексные задачи объемно-календарного планирования // Известия РАН. Теория и системы управления. — 2007. — № 1. — С. 78–82.

4. Прилуцкий М. Х. Многокритериальное распределение однородного ресурса в иерархических системах // Автоматика и телемеханика. — 1996. — № 2. — С. 139–146.

О МОЩНОСТИ БАЗИСОВ КОНСТРУКТИВНЫХ ОПИСАНИЙ ГРАФОВ

Е. В. Бурков (Нижний Новгород)

В работе исследуются конструктивные описания графов [1]. На множестве всех графов $\Im$ рассматривается многозначная бинарная

операция $\phi : \Im \times \Im \to \Im$, определяющаяся тернарным отношением $\phi' \subseteq \Im \times \Im \times \Im$: $G_1 \phi G_2 \to G \Leftrightarrow (G_1, G_2, G) \in \phi'$. Отношение $\phi' \subseteq \Im \times \Im \times \Im$ определяет *бинарную операцию склейки*, если для любых $(G_1, G_2, G) \in \phi'$ *результирующий граф* G допускает представление в виде объединения с пересечением подграфов, изоморфных *графам-операндам* G_1 и G_2. Это пересечение $\tilde{G}$, изоморфное подграфам $G_1' \subseteq G_1$ и $G_2' \subseteq G_2$, $G_1' \cong G_2'$, называется *подграфом склейки*, а отношение ϕ' *отношением склейки*. Если не указано иное, считаем, что отношение склейки включает все возможные тройки графов, удовлетворяющие этому условию.

Операция склейки ϕ *удовлетворяет системе ограничений* $H \subseteq \Im \times \Im \times \Im$, если соответствующее отношение $\phi' \subseteq H$. В этом случае операцию ϕ называем *операцией H-склейки*.

Ограничение H_S на вид подграфа склейки определяется множеством $H_S' = \{H_1, H_2, \ldots\}$ допустимых подграфов склейки и включает в себя такие тройки (G_1, G_2, G), что граф G допускает представление в виде объединения с пересечением подграфов, изоморфных G_1 и G_2, при котором подграф склейки изоморфен некоторому $H_i \in H_S'$.

Пусть $P \subseteq \Im$ — класс графов, обладающих некоторым характеристическим свойством.

Систему ограничений $H = \{(G_1, G_2, G) | G_1, G_2, G \in P\}$ называем *естественной системой ограничений*. Естественная система ограничений обеспечивает сохранение заданного свойства графов-операндов. Отношение склейки $\phi'_H = \phi' \cap H$ называем *естественным отношением склейки* для класса P.

Граф G является *H-суперпозицией* графов из P, если $G \in P$ или G может быть получен из графов множества P с помощью операций H-склейки. Множество $[P]_H$ всех графов, являющихся H-суперпозицией графов из P, образует *H-замыкание* P. Если $[P]_H = P$, то P является *H-замкнутым* классом графов.

Минимальное по включению подмножество B_e графов из P образует *элементный базис* H-замкнутого класса P, если $[B_e]_H = P$.

Минимальное по включению множество $B_o = \{H_1, H_2, \ldots\}$, определяющее ограничение H_S на вид подграфа склейки, при котором $[B_e]_{H \cap H_S} = P$, называется *операционным базисом* H-замкнутого класса P.

Совокупность системы ограничений H, элементного базиса B_e и операционного базиса B_o образует *конструктивное описание* H-замкнутого класса P.

Доказано, что для любого *H-замкнутого* класса графов P су-

ществует единственный элементный базис B_e [1] и по крайней мере один операционный базис B_o [2]. В [1] приведены примеры классов графов, имеющих конечные элементный и операционный базисы. Известен класс графов, имеющий бесконечный элементный базис и по крайней мере три различных конечных операционных базиса [3, 4], а также класс графов, имеющий бесконечные элементный и операционный базисы [5]. Выполнимость последней оставшейся логической возможности показывает следующая

Теорема. *Существует класс графов с конечным элементным и бесконечным операционным базисом.*

Доказательство. Рассмотрим класс графов $P = \{L_i | i \geq 1\} \cup \{C_i | i \geq 2\} \cup \{C_i^2 | i \geq 2\}$, где L_i — простая цепь из i ребер, C_i — простой цикл длины i, C_i^2 — цикл длины i, составленный из кратных ребер.

Естественное отношение склейки для класса P выглядит так: $\phi'_H = \{(L_i, L_j, L_k) | i, j \geq 1, \max(i, j) \leq k \leq i + j\} \cup \{(L_i, L_j, C_k) | i, j \geq 1, \max(i, j) + 1 \leq k \leq i + j\} \cup \{(C_i, C_i, C_i^2) | i \geq 2\}$.

Элементный базис H-замкнутого класса P состоит из одного элемента $B_e = \{L_1\}$. Действительно, из L_1 последовательными склейками по подграфу K_1 можно получить цепь L_i любой длины, любой цикл $C_i, i \geq 2$ получается из L_{i-1} и L_1 склейкой по пустому графу $\bar{K}_2$, и, наконец, любой двойной цикл C_i^2 получается из двух C_i склейкой по $\bar{K}_i$. Так как построение графа C_i^2 невозможно без склейки по подграфу $\bar{K}_i$, в операционный базис класса P входят все пустые графы $\bar{K}_i, i = 2, 3, \ldots$. Следовательно, операционный базис класса P счетный.

Список литературы

1. Иорданский М. А. Конструктивные описания графов // Дискретный анализ и исследование операций. — 1996. — Т. 3, № 4. — С. 33–63.

2. Бурков Е. В. Операционные базисы замкнутых классов графов // Материалы IX международного семинара "Дискретная математика и ее приложения", посвященного 75-летию со дня рождения академика О. Б. Лупанова (18–23 июня 2007 г.). — М.: Изд-во механико-математического факультета МГУ, 2007. — С. 261–263.

3. Иорданский М. А., Бурков Е. В. Конструктивные описания эйлеровых планарных графов // VI Международная конференция "Дискретные модели в теории управляющих систем" (7–11 декабря 2004 г.). — М., 2004. — С. 167–169.

4. Бурков Е. В. Еще один операционный базис класса эйлеровых планарных графов // XV международная конференция "Проблемы

теоретической кибернетики" (2–7 июня 2008 г.). — Казань: Отечество, 2008. — С. 13.

5. Иорданский М. А. Счетный операционный базис топологических эйлеровых планарных графов // VIII Международная конференция "Дискретные модели в теории управляющих систем" (6–9 апреля 2009 г.). — М., 2009. — С. 127–129.

ИНТЕГРАЛЬНОЕ ПРЕДСТАВЛЕНИЕ ДЛЯ ЧИСЛА ПОМЕЧЕННЫХ КУБИЧЕСКИХ ГРАФОВ

В. А. Воблый (Москва)

Пусть C_n — число простых кубических графов с $2n$ помеченными вершинами. Рид [1] получил формулу

$$C_n = \frac{(2n)!}{6^n} \sum_{i=0}^{n} \sum_{j=0}^{2i} \frac{(-1)^j (6i-2j)! 6^j A_{-1}(j)}{(3i-j)!(2i-j)! j! (n-i)! 48^i},$$

$$A_p(q) = \sum_{k=0}^{[\frac{q}{2}]} \frac{p^k q!}{(q-2k)! k!}.$$

Теорема 1. *Число C_n имеет интегральное представление*

$$C_n = \frac{1}{\sqrt{\pi} 6^n} \int_0^\infty \frac{e^{-t}}{\sqrt{t}} (3t-1)^n H_{2n}\left(\left(\frac{t}{3} - \frac{1}{2}\right)\sqrt{\frac{3t}{3t-1}}\right) dt,$$

где $H_n(x)$ — многочлен Эрмита.

Доказательство. С учетом формулы удвоения для гамма-функции и выражения для многочленов Эрмита имеем:

$$\frac{(6i-2j)!}{(3i-j)!} = \frac{1}{\sqrt{\pi}} 2^{6i-2j} \Gamma(3i-j+\frac{1}{2}), \quad (-1)^j A_{-1}(j) = H_j(-\frac{1}{2}).$$

Используя интегральное представление для гамма-функции и тождество для многочленов Эрмита [3, с. 640]:

$$\sum_{j=0}^{\infty} \binom{m}{j} u^j H_j(x) = u^m H_m(x + \frac{1}{2u}),$$

получим

$$C_n = \frac{(2n)!}{\sqrt{\pi}6^n}\sum_{i=0}^{n}\frac{(4/3)^i}{(2i)!(n-i)!}\times$$
$$\times\int_0^\infty e^{-t}t^{3t-1/2}\sum_{j=0}^{2i}\binom{2i}{j}\left(\frac{3}{2t}\right)^j H_j\left(-\frac{1}{2}\right)dt =$$
$$= \frac{(2n)!}{\sqrt{\pi}6^n}\int_0^\infty\frac{e^{-t}}{\sqrt{t}}\sum_{i=0}^{n}\frac{(3t)^i}{(2i)!(n-i)!}H_{2i}\left(\frac{t}{3}-\frac{1}{2}\right)dt.$$

С помощью другого тождества для многочленов Эрмита [3, с. 640]:

$$\sum_{i=0}^{n}\frac{w^i H_{2i}(x)}{(2i)!(n-i)!} = \frac{(w-1)^n}{(2n)!}H_{2n}\left(x\sqrt{\frac{w}{w-1}}\right)$$

завершим доказательство теоремы.

Обозначим

$$C_n(m) = \frac{1}{\sqrt{\pi}2^n}\int_0^\infty e^{-t}t^{n-1/2}\left(\sqrt{1-\frac{1}{3t}}\right)^m\times$$
$$\times H_m\left(\left(\frac{t}{3}-\frac{1}{2}\right)\sqrt{\frac{3t}{3t-1}}\right)dt,$$

Теорема 2. *Пусть* $F(u,v) = \sum_{n=0}^{\infty}\sum_{m=0}^{\infty}C_n(m)\frac{u^n v^m}{n!m!}$ *— производящая функция для чисел* $C_n(m)$*, тогда верно равенство*

$$F(u,v) = \frac{1}{\sqrt{1-u/2-2v/3}}\exp(-v^2-v-\frac{2}{3}\sqrt{2v^3-3v^2(1-u/2)}).$$

Доказательство. Подставим в $F(u,v)$ выражение для $C_n(m)$ и поменяем местами знаки интегрирования и суммирования

$$F(u,v) = \tfrac{1}{\sqrt{\pi}}\int_0^\infty\tfrac{e^{-t}}{\sqrt{t}}\sum_{n=0}^{\infty}\tfrac{(tu/2)^n}{n!}\times$$
$$\times\sum_{m=0}^{\infty}(v\sqrt{1-1/3t})^m H_m\left(\frac{t/3-1/2}{\sqrt{1-1/3t}}\right)dt.$$

С помощью производящей функции для многочленов Эрмита и разложения в степенной ряд для экспоненты получим

$$F(u,v) = \frac{1}{\sqrt{\pi}} e^{-v^2-v} \int_0^\infty exp(-t(1-u/2-2v/3)+v^2/3t)\frac{dt}{\sqrt{t}}.$$

В силу известного интеграла [2, с. 344]

$$\int_0^\infty e^{-px-q/x}\frac{dx}{\sqrt{x}} = \sqrt{\frac{\pi}{p}}e^{-2\sqrt{pq}}, \quad \Re p > 0, \quad \Re q > 0,$$

получим утверждение теоремы.

Теорема 3. *При $n \to \infty$ верна асимптотика*

$$C_n \sim \frac{e^{-2}}{2\pi n}\left(\frac{3}{2}\right)^n n!(2n)!$$

Очевидно, $C_n = C_n(2n)$. При доказательстве этой теоремы для получения асимптотики $C_n(m)$ при $n \to \infty$ и $m \to \infty$ используется теорема Бендера [4, теорема 3], а также ее обобщение, данное в работе Бендера и Ричмонда [5].

Отметим, что асимптотика для числа C_n при $n \to \infty$ получена еще Ридом [6, с. 209] в виде: $C_n \sim \frac{e^{-2}(6n)!}{288^n(3n)!}$.

С помощью формулы Стирлинга для факториала можно показать, что асимптотика Рида совпадает с асимптотикой, полученной в теореме 3.

Список литературы

1. Read R. C. The enumeration of locally restricted graphs. I // J. London Math. Soc. — 1959. — V. 34. — P. 417–436.

2. Прудников А. П. и др. Интегралы и ряды. Т. 1. — М.: Наука, ГРФМЛ, 1981.

3. Прудников А. П. и др. Интегралы и ряды. Т. 2. — М.: Наука, ГРФМЛ, 1983.

4. Bender E. A. Central and local limits theorems applied to asymptotic enumeration // J. Combin. Theory. — 1973. — A15. — P. 91–111.

5. Bender E. A., Richmond L. B. Central and local limits theorems applied to asymptotic enumeration. II. Multivariate generating functions. — J. Combin. Theory. — 1983. — A34. — P. 255–265.

6. Харари Ф., Палмер Э. Перечисление графов. — М.: Мир, 1979.

О РЕАЛИЗАЦИИ НАТУРАЛЬНЫХ ЧИСЕЛ ИНВАРИАНТАМИ ГРАФОВ

А. Б. Дайняк (Москва)

Значительное место в теории графов занимают задачи, связанные с оценкой различных инвариантов графа, например, хроматического числа, кликового числа, количества независимых множеств и др. Во многих случаях интерес представляет и обратная задача: найти граф (если он существует), заданный инвариант которого принимает заданное значение (см., например, [2]). Классическим примером является задача определения для заданного набора целых неотрицательных чисел, соответствует ли этот набор степеням вершин некоторого графа [1, гл. 8].

В самом общем виде задачу можно поставить следующим образом. Пусть $\mathcal{G}$ — класс графов, а $\phi : \mathcal{G} \to S$ и $\psi : \mathcal{G} \to T$ — заданные на этом классе функционалы. Задача существования ставится так: "для всякого ли $s \in S$ найдётся граф $G \in \mathcal{G}$, такой, что $\phi(G) = s$?" Если ответ на предыдущий вопрос положителен, то имеет смысл задача минимизации: "для заданного $s \in S$ найти величину $L(s) = \inf\{\psi(G) \mid G \in \mathcal{G}, \phi(G) = s\}$". В работе [3] была решена задача существования в случае, когда $\mathcal{G}$ — класс всех двудольных графов, а ϕ — количество независимых множеств вершин графа.

В данной работе в качестве $\mathcal{G}$ мы также рассматриваем класс двудольных графов, а в качестве ϕ — количество *максимальных по включению* независимых множеств (м. н. м.). В этом случае вопрос существования соответствующего графа тривиален: произвольное натуральное число $n \geq 4$ можно реализовать как число м. н. м. в *графе-короне*, получающимся отбрасыванием рёбер совершенного паросочетания из полного двудольного графа $K_{n-2,n-2}$. Рассматривая в качестве ψ число вершин графа, мы приходим к задаче оптимизации: "для натурального n найти минимальное число $L(n)$, такое, что существует двудольный граф с числом вершин $L(n)$ и количеством м. н. м., равным n". Из того, что число м. н. м. в двудольном графе не превосходит числа подмножеств любой из его долей, вытекает

Утверждение. *Для любого* $n \in \mathbb{N}$ *имеем* $L(n) \geqslant \log_2 n$.

Для получения верхней оценки $L(n)$ доказывается следующая

Лемма 1. *Пусть* G *—двудольный граф, для которого* $\phi(G) = k$, $\psi(G) = n$. *Тогда существуют графы* $G_1, \ldots, G_5$, *такие, что* $\phi(G_1) = 2k$, $\phi(G_2) = 3k$, $\phi(G_3) = 6k + 1$, $\phi(G_4) = 6k + 3$, $\phi(G_5) = 6k+5$, $\psi(G_1) = n+2$, $\psi(G_2) = n+4$, $\psi(G_3) = \psi(G_4) = \psi(G_5) = n+8$.

Индукцией по n, с использованием леммы 1, доказывается

Теорема 1. $L(n) \leqslant 8 \log_6 n < 3.1 \log_2 n$.

Лемма 2. *Пусть G и $\tilde{G}$ — двудольные графы без изолированных вершин, и пусть $m, t \in \mathbb{N}$. Тогда найдётся двудольный граф G', такой, что*

$$\phi(G') = 2^{mt} \cdot \phi(G) + \frac{2^{mt} - 1}{2^t - 1} \cdot \phi(\tilde{G}) - 2$$

и $\psi(G') = \psi(G) + \psi(\tilde{G}) + 2m(t+1) - 1$.

Из теоремы 1 и леммы 2 выводится следующая

Лемма 3. *Пусть G —двудольный граф, и пусть $m, t \in \mathbb{N}$. Тогда найдётся двудольный граф G', такой, что*

$$\phi(G') = 2^{mt} \cdot (\phi(G) + 1) - 1$$

и $\psi(G') \leqslant \psi(G) + 2mt + 2m + 4t - 1$.

Для натурального n обозначим через $A(n)$ количество отрезков из идущих подряд единиц в двоичной записи n. С использованием леммы 3 индукцией по n доказывается

Теорема 2. *Пусть n — натуральное число, такое, что $A(n) = o(\log n)$. Тогда $L(n) \sim 2 \log_2 n$.*

В заключение сформулируем естественную гипотезу:

Предположение. *Имеет место асимптотика $L(n) \sim 2 \log_2 n$ для любого n.*

Работа поддержана РФФИ, проект 10-01-00768-а.

Список литературы

1. Емеличев В. А., Мельников О. И., Сарванов В. И., Тышкевич Р. И. Лекции по теории графов. — М.: Книжный дом "Либроком", 2009.

2. Czabarka E., Szekely L., Wagner S. The inverse problem for certain tree parameters // Discrete Applied Mathematics. — 2009. — V. 15 (157). — P. 3314–3319.

3. Linek V. Bipartite graphs can have any number of independent sets // Discrete Mathematics. — 1989. — V. 2 (76). — P. 131–136.

ПОСТРОЕНИЕ T-ФАКТОРИЗАЦИЙ ПОЛНОГО ГРАФА И ПРОБЛЕМА РОСА

Г. А. Донец, Д. А. Петренюк (Киев)

Разложением графа H на подграфы из данного семейства $G = g_1, \ldots, g_k$, или (H, G)-*разложением* называется разбиение множества ребер графа H на подграфы (*компоненты разложения*), каждый из которых изоморфен одному из элементов множества G. Возникает *задача существования*: существуют ли (H, G)-разложения для данного графа H и множества G? В зависимости от типов H и G получим положительный ответ только в том случае, если будет решена задача построения, т. е. будет построено (H, G)-разложение. Подграф G_i называется фактором графа G, если множество вершин подграфа G_i совпадает с множеством вершин графа G. Факторизацией графа называется такое разложение графа, компонентами которого являются факторы данного графа. В качестве основного графа служит, как правило, полный n-вершинный граф $G = K_n$. Факторизацию полного графа, все компоненты которой изоморфны некоторому дереву T, называют T-*факторизацией. Полусимметричным* деревом будем называть дерево порядка $n = 2k$, которое содержит центральное ребро и допускает изоморфизм, переставляющий концы центрального ребра. Очевидно, что после удаления центрального ребра полусимметричное дерево распадается на две изоморфные связные компоненты — симметричные половины. Их можно рассматривать как корневые деревья, корни которых – концы центрального ребра соответствующего полусимметричного дерева. Как видим, существует взаимно однозначное соответствие между полусимметричным деревом и его симметричной половиной. Одним из основных методов построения T-факторизации полусимметричных деревьев является *полуоборотный метод*. T-факторизации деревьев, полученные с помощью этого метода, также будем называть полуоборотными. Идея этого метода состоит в использовании шаблона, представляющего собой окружность, поделенную $n = 2k$ точками на равные дуги (назовем эти дуги *элементарными*). Точки деления последовательно занумеруем $1, \ldots, n$. Под длиною хорды будем подразумевать количество элементарных дуг в меньшей из дуг, на которые эта хорда разбивает окружность. Полусимметричное дерево T порядка $n = 2k$ называют правильно вписанным в эту окружность, если: а) точки деления являются вершинами дерева T; б) ребра дерева T изображаются хордами окружности; в) для каждой допустимой длины хорды ровно два нецентральных ребра, симметричных относительно центра окружности, имеют такую длину. Если T полусимметричное дерево порядка $n = 2k$, правиль-

но вписанное в окружность, то можно выполнить T-факторизацию графа K_n на k компонент, изоморфных дереву T. Факторизация выполняется поворотом первой компоненты (дерева T_1) вокруг центра окружности, т. е. увеличением всех номеров вершин первой компоненты на 1 (mod n). Повороты осуществляются до тех пор, пока дерево T_1 не повернется на полкруга. Отсюда и название метода. Таким образом, задача построения T-факторизации сводится к правильному вписыванию дерева в шаблон. Принимая во внимание то, что полусимметричное дерево однозначно определяется своей половиной, последнюю задачу можно свести к вписыванию половины дерева в полуокружность. Нетрудно убедиться в том, что для успешного решения задачи правильного вписывания k-вершинного дерева в полуокружность необходимо так занумеровать его вершины числами $x_i \in (1, \ldots, k)$, чтобы абсолютные разности кодов смежных вершин составляли множество $(1, \ldots, k-1)$. Эта задача носит название проблемы А. Роса. Приведем некоторые определения и результаты. Всякую нумерацию k-вершинного дерева, которая решает проблему А. Роса, будем называть *правильной* и обозначать $X = (x_1, \ldots, x_k) \in N_x$.

Утверждение 1. Всякой правильной нумерации дерева соответствует другая (двойственная) нумерация $X\prime = (x\prime_1, \ldots, x\prime_k)$, которая получается после перекодирования вершин $X\prime_i = k+1-x_i$ $(1 \le i \le k)$.

Утверждение 2. Произвольная k-вершинная звезда допускает правильную нумерацию, если центральной вершине присвоить код 1 (или k для двойственной нумерации).

Утверждение 3. Произвольная k-вершинная цепь допускает правильную нумерацию.

Доказательство можно провести по индукции. Рассмотрим еще одну разновидность дерева, которая называется *гусеницей*. Это такое дерево, которое после удаления в нем висячих вершин (вершины со степенью 1) превращается в цепь. Эту цепь назвать стволом дерева, а висячие вершины – листьями дерева, произрастающими из вершин ствола.

Утверждение 4. Гусеница допускает правильную нумерацию вершин.

Она обладает замечательным свойством, которое можно использовать при композиции нескольких деревьев.

Утверждение 5. Если к вершине с кодом 1 правильно занумерованного дерева присоединить гусеницу, то полученное дерево допускает правильную нумерацию.

Теорема 1. *Полусимметричное дерево с числом вершин* 18 *допускает T-факторизацию.*

Непосредственно можно убедиться, что большинство деревьев

порядка 9 представляют собой гусеницы. Из оставшихся деревьев все, за исключением двух, представляют собой композицию цепи с числом вершин 5 или 6 и гусеницы. На каждой из этих цепей необходимо построить правильную нумерацию $f_5(3)$ или $f_6(3)$, что выполняется достаточно легко. Для двух оставшихся деревьев правильная нумерация найдена "вручную", путем перебора.

Теорема 2. *Полусимметричное дерево с числом вершин* 20 *допускает* T*-факторизацию.*

Этот метод можно применять и для деревьев более высокого порядка. На определенном уровне придется прибегнуть к помощи вычислительной техники. Непосредственное использование вычислительной техники для простого перебора вариантов уже для деревьев порядка 20–22 наталкивается на существенные препятствия технического характера.

Список литературы

1. Петренюк А. Я. Екстремальні розклади повних графів: існування, перелік. — Дис. д-ра фіз.-мат. наук: 01.05.01. – К., 2002.

ОСЛАБЛЕННЫЙ ЗАКОН НУЛЯ ИЛИ ЕДИНИЦЫ ДЛЯ СЛУЧАЙНЫХ ДИСТАНЦИОННЫХ ГРАФОВ

М. Е. Жуковский (Москва)

В 1960 году А. Эренфойхт [1] доказал теорему о структурах, определенных с помощью формул первого порядка [2].

Теорема 1. *Пусть* ϕ *— замкнутая формула первого порядка. Она определяет класс структур* $\mathcal{C}$ *над сигнатурой* S*. Существует такое* k*, что если* $\mathcal{A} \in \mathcal{C}$ *и* $\mathcal{B} \notin \mathcal{C}$*, то у Новатора есть выигрышная стратегия в игре* $EHR(\mathcal{A}, \mathcal{B}, k)$.

Случайный граф $G(N,p)$ (см. [3]) подчиняется *закону нуля или единицы* [4–7], если для любого свойства L первого порядка выполняется одно из двух условий: либо $\lim\limits_{N\to\infty} \mathcal{P}_{N,p}(G \vDash L) = 0$, либо $\lim\limits_{N\to\infty} \mathcal{P}_{N,p}(G \vDash L) = 1$. На основе теоремы 1 в 1969 году Ю. В. Глебский, Д. И. Коган, М. И. Лиогонький и В. А. Таланов [4] получили следующий закон нуля или единицы, который в 1976 году был независимо доказан Р. Фагиным [5].

Теорема 2. *Пусть функция $p = p(N)$ такова, что $pN^\alpha \to \infty$ при $N \to \infty$ и $(1-p)N^\alpha \to \infty$ при $N \to \infty$ для любого $\alpha > 0$, тогда случайный граф подчиняется закону нуля или единицы.*

Также в статье [6] С. Шела и Дж. Спенсера описан результат, в котором расширен класс функций, подчиняющихся закону нуля или единицы.

Теорема 3. *Пусть $p(N) = N^{-\alpha}$, где α — иррациональное, $0 < \alpha < 1$, тогда случайный граф подчиняется закону нуля или единицы.*

Пусть фиксированы $j \in \mathbb{N}$ и сигнатура $S = (R_1, ..., R_s)$. Будем рассматривать формулы над сигнатурой S, построенные с помощью символов из S; символа отношения $=$; логических связок $\neg, \Rightarrow, \Leftrightarrow, \vee, \wedge$; переменных $x, y, x_1...$; кванторов $\forall$, $\exists$, причем если количество кванторов больше, чем j, то в формуле не могут присутствовать различные кванторы. Будем обозначать такую формулу ϕ_j.

Пусть $\mathcal{A}$ и $\mathcal{B}$ — две S-структуры. Определим *ослабленную j-игру Эренфойхта* $EHR_j(\mathcal{A}, \mathcal{B}, k)$ с фиксированным числом раундов k и двумя игроками, Новатором и Консерватором. Она будет отличаться от игры $EHR(\mathcal{A}, \mathcal{B}, k)$ только тем, что если $k > j$, то Новатор не имеет права в каждом раунде выбирать структуру. Он волен выбирать структуру, из которой впоследствии будет выбирать элементы, только в первом раунде. Во всех последующих раундах он обязан выбирать элемент только из выбранной в первом раунде структуры. Если $k \leq j$, то правила игры остаются прежними.

Пусть $k \in \mathbb{N}$, $n = 4k$. Положим $N = C_n^{n/2}$. Рассмотрим граф $G_N^{dist} = (V_N^{dist}, E_N^{dist})$, в котором $V_N^{dist} = \{\mathbf{x} = (x_1, ..., x_n) : \ x_i \in \{0,1\}, \ \sum\limits_{i=1}^{n} x_i = n/2\}$; $E_N^{dist} = \left\{\{\mathbf{x}, \mathbf{y}\} \in V_N^{dist} \times V_N^{dist} : \sum\limits_{i=1}^{n} x_i y_i = k\right\}$. Такой граф называется *дистанционным* [8].

В настоящей работе мы будем рассматривать *случайные дистанционные графы* $G(G_N^{dist}, p)$. Здесь $G(G_N^{dist}, p)$ — это вероятностное пространство $G(G_N^{dist}, p) = \left(\Omega_{G_N^{dist}}, \mathcal{F}_{G_N^{dist}}, \mathcal{P}_{G_N^{dist}, p}\right)$, где

$$\Omega_{G_N^{dist}} = \{\mathcal{G}_N^0 = (\mathcal{V}_N^0, \mathcal{E}_N^0) : \ \mathcal{V}_N^0 = \mathcal{V}_N, \ \mathcal{E}_N^0 \subseteq \mathcal{E}_N\},$$

$$\mathcal{F}_{G_N^{dist}} = 2^{\Omega_{G_N^{dist}}},$$

$$\mathcal{P}_{G_N^{dist}, p}(\mathcal{G}_N^0) = p^{|\mathcal{E}_N^0|}(1-p)^{|G_N^{dist}| - |\mathcal{E}_N^0|}.$$

Пусть $\{\mathcal{G}_{N_i}\}_{i \in \mathbb{N}}$ — последовательность неориентированных графов без петель и кратных ребер, $|V(\mathcal{G}_{N_i})| = N_i$. Будем говорить,

что *последовательность случайных графов* $\{G(\mathcal{G}_{N_i}, p(N_i))\}_{i\in\mathbb{N}}$ *подчиняется ослабленному* j*-закону нуля или единицы*, если для любого свойства L_j, определенного замкнутой формулой ϕ_j, выполняется одно из двух условий: либо $\lim\limits_{i\to\infty} \mathcal{P}_{\mathcal{G}_{N_i},p}(\mathcal{G} \models L_j) = 0$, либо $\lim\limits_{i\to\infty} \mathcal{P}_{\mathcal{G}_{N_i},p}(\mathcal{G} \models L_j) = 1$. Будем говорить, что *случайный дистанционный граф подчиняется ослабленному* j*-закону нуля или единицы,* если этому закону подчиняется последовательность случайных графов $\{G(G^{dist}_{N(k)}, p(N(k)))\}_{k\in\mathbb{N}}$.

Сформулируем теперь наши результаты.

Теорема 4. *Пусть* j *— фиксированное натуральное число. Пусть также* $\mathcal{C}$ *— класс структур над некоторой сигнатурой* S*, определяемый замкнутой формулой* ϕ_j*. Существует такое* k*, что если* $\mathcal{A} \in \mathcal{C}$ *и* $\mathcal{B} \notin \mathcal{C}$*, то у Новатора есть выигрышная стратегия в игре* $EHR_j(\mathcal{A}, \mathcal{B}, k)$.

Теорема 5. *Пусть функция* $p = p(N)$ *такова, что* $pN^\alpha \to \infty$ *при* $N \to \infty$ *и* $(1-p)N^\alpha \to \infty$ *при* $N \to \infty$ *для любого* $\alpha > 0$*. Тогда для случайных дистанционных графов выполнен ослабленный* 3*-закон нуля или единицы.*

Теорема 6. *Пусть функция* $p = p(N)$ *такова, что* $pN^\alpha \to \infty$ *при* $N \to \infty$ *и* $(1-p)N^\alpha \to \infty$ *при* $N \to \infty$ *для любого* $\alpha > 0$*. Пусть также фиксировано* $k \in \{2, 3\}$ *и последовательность* $\{n_i\}_{i\in\mathbb{N}}$ *определена следующим образом:* $n_i = 4k!i$*. Рассмотрим произвольную последовательность натуральных чисел* $\{m_i\}_{i\in\mathbb{N}}$*, которая удовлетворяет следующему условию:*

$$\forall i\, \exists j_1, j_2\ ((j_1 > i) \wedge (j_2 > i) \wedge (4(k-1)!|m_i) \wedge (\neg(4k!|m_{j_1})) \wedge (4k!|m_{j_2})).$$

Рассмотрим, наконец, произвольную последовательность $\{t_i\}_{i\in\mathbb{N}}$ *вида* $t_i = 4k!i + 4(k-1)!j$*, где при каждом* i *величина* j *— это любое число из множества* $\{1, ..., k-1\}$.

Для любого натурального i *определим* $N_i = C_{n_i}^{n_i/2}$, $M_i = C_{m_i}^{m_i/2}$, $T_i = C_{t_i}^{t_i/2}$*. Тогда для последовательностей случайных дистанционных графов* $\{G(G^{dist}_{N_i}, p)\}_{i\in\mathbb{N}}$, $\{G(G^{dist}_{T_i}, p)\}_{i\in\mathbb{N}}$ *выполняется ослабленный* $(k+2)$*-закон нуля или единицы, а для последовательности случайных дистанционных графов* $\{G(G^{dist}_{M_i}, p)\}_{i\in\mathbb{N}}$ *ослабленный* $(k+2)$*-закон нуля или единицы не выполняется.*

Список литературы

1. Ehrenfeucht A. An application of games to the completness problem for formalized theories // Fund. Math. — Warszawa, 1960. — 49. —

С. 121–149.
2. Верещагин Н. К., Шень А. Языки и исчисления. —М.: МЦНМО, 2000.
3. Bollobas B. Random Graphs. — New York: Academic Press, 1985.
4. Глебский Ю. В., Коган Д. И., Лиогонький М. И., Таланов В. А. Объем и доля выполнимости формул узкого исчисления предикатов // Кибернетика. — 1969. — № 2. — С. 17–27.
5. Fagin R. Probabilities in finite models // J. Symbolic Logic — 1976. — 41. — С. 50–58.
6. Shelah S., Spencer J. H. Zero-one laws for sparse random graphs // J. Amer. Math. Soc. — 1988. — 1. — С. 97–115.
7. Спенсер Дж., Алон Н. Вероятностный метод. —М.: БИНОМ. Лаборатория знаний, 2007.
8. Райгородский А. М. Проблема Борсука и хроматические числа метрических пространств // Успехи матем. наук. — 2001. — № 1 (56). — С. 107–146.

ОЦЕНКА ЧИСЛА ГРАФОВ В НЕКОТОРЫХ НАСЛЕДСТВЕННЫХ КЛАССАХ

В. А. Замараев (Нижний Новгород)

Рассматриваются бесконечные наследственные классы графов. Множество X называется наследственным классом графов, если любой граф, изоморфный порожденному подграфу графа из X, также принадлежит X. Все графы являются помеченными, с множеством вершин $\{1, 2, \ldots, n\}$. Известно, что любой наследственнй класс графов X можно определить с помощью множества M запрещённых подграфов, при этом принято писать, что $X = Free(M)$. В [1] доказано, что для любого бесконечного наследственного класса графов, отличного от класса всех графов, справедливо:

$$\log_2 |X_n| = \left(1 - \frac{1}{c(X)}\right) \frac{n^2}{2} + o(n^2), \qquad (1)$$

где $c(X)$ — натуральное число, называемое индексом класса X и определенное в [1]. При этом множество всех бесконечных наследственных классов графов, отличных от класса всех графов, разбивается на слои, где каждому слою принадлежат классы с одним и тем же значением индекса. Например, множество классов, которым

соответствует индекс, равный единице, называется унитарным слоем. В [1] описаны также минимальные классы каждого слоя. Например, при $c = 2$ имеется только три минимальных класса: класс двудольных графов, класс графов, дополнительных к двудольным (кодвудольных), и класс расщепляемых графов. Таким образом, унитарный слой может быть охарактеризован как слой, состоящий из тех и только тех бесконечных наследственных классов, которые не содержат ни одного из трех перечисленных. Унитарный слой представляет особый интерес, так как при $c = 1$ соотношение (1) не даёт асимптотики для величины $\log_2 |X_n|$, знание которой важно, например, при экономном кодировании графов из класса X [2]. В то же время этому слою принадлежат многие известные классы: леса, планарные графы, рёберные графы, интервальные графы, кографы и др. Целью данного исследования является изучение классов графов из унитарного слоя, определяемых не более чем тремя запрещёнными подграфами. Так как классы принадлежат слою с индексом, равным единице, то в множестве запрещённых графов должно быть хотя бы по одному представителю из класса двудольных, класса кодвудольных и класса расщепляемых графов. Если запрещённый подграф один, то такой подграф должен быть двудольным, кодвудольным и расщепляемым. Всего имеется шесть графов, удовлетворющих этим требованиям, все они являются порождёнными подграфами графа P_4. Класс $Free(P_4)$ хорошо изучен. Далее логично поставить вопрос о характеристиках классов из унитарного слоя, определяемых двумя запрещёнными подграфами. В этом случае один из запрещённых подграфов должен принадлежать одновременно двум классам. На текущем этапе исследований рассматриваются классы, у которых один запрещённый подграф двудольный и расщепляемый, а второй — полный (являющийся кодвудольным). В частности, в данной работе даётся оценка числа n-вершинных графов в классах $Free(K_{1,s}+O_p, K_q)$. Заметим, что число n-вершинных графов в классе $M_{s,p,q} = Free(K_{1,s} + O_p, K_q)$ не превосходит числа n-вершинных графов в классе $M_{t,t,t} = N_t$, где $t = \max\{s, p, q\}$. Если мы получим верхнюю оценку для числа n-вершинных графов в классе N_t, то эта же оценка будет справедлива и для класса $M_{s,p,q}$. Поэтому здесь рассматриваются только классы N_t, это позволяет уменьшить количество используемых индексов. Далее используются следующие обозначения. Подграф графа G, порождённый множеством вершин $A \subseteq V(G)$, обозначается через $G[A]$. Через $R(q, p)$ обозначается число Рамсея с параметрами q и p, то есть такое наименьшее число, что всякий граф с числом вершин не менее $R(q, p)$ содержит либо K_q, либо O_p в качестве порождённого подграфа. Доказательство главного

результата данной работы основано на следующей лемме.

Лемма. *Пусть G — некоторый n-вершинный граф из класса $Free(K_{1,p}+O_p, K_p)$, $p \geq 2$. Существует разбиение $V(G) = A_1 \cup \cdots \cup A_r \cup C$ множества вершин графа G со следующими свойствами:*

1) $r < R(R(p,p)+1, p)$;

2) $|A_i| \geq d$, *где* $i = \overline{1,r}$, $d = p2^{p-1} + 2p(p-1) + 1$;

3) A_i *порождает пустой подграф,* $i = \overline{1,r}$;

4) $G[C] \in Free(O_d, K_p)$.

Основной результат сформулируем в виде теоремы.

Теорема. *Для любого p, $p \geq 2$, число n-вершинных графов в классе N_p не превосходит n^{cn}, где c — некоторая константа, зависящая только от p.*

Список литературы

1. Алексеев В. Е. Область значений энтропии наследственных классов графов // Дискретная математика. — 1992. — Т. 4, вып. 2. — С. 148–157.

2. Алексеев В. Е. Наследственные классы и кодирование графов // Проблемы кибернетики. Вып. 39. — М.: Наука, 1982. — С. 151–164.

ВЗВЕШЕННЫЕ НЕЗАВИСИМЫЕ МНОЖЕСТВА В ГРАФАХ С ОГРАНИЧЕННЫМИ МИНОРАМИ РАСШИРЕННОЙ МАТРИЦЫ ИНЦИДЕНТНОСТИ

Д. В. Захарова (Нижний Новгород)

В задаче о взвешенном независимом множестве (ВНМ) дан граф с приписанными его вершинам положительными целыми весами, и требуется найти множество попарно несмежных вершин с наибольшим суммарным весом. Пусть w_i — вес вершины i, $i = 1, 2, \ldots, n$. Задача ВНМ может быть сформулирована как задача целочисленного линейного программирования: найти целочисленный вектор $(x_1, x_2, \ldots, x_n)$, максимизирующий величину $\sum w_i x_i$ при ограничениях $x_i + x_j \leq 1$ для каждого ребра (i, j) и $x_i \geq 0$, $i = 1, \ldots, n$. Матрица этой задачи — транспонированная матрица инцидентности графа. В. Н. Шевченко [2] предположил, что для любой константы

$c > 0$ задача целочисленного линейного программирования, у которой абсолютные величины миноров матрицы ограничений не превосходят c, решается за полиномиальное время. В ослабленных вариантах этой гипотезы фигурируют расширенные матрицы, получающиеся добавлением столбца правых частей неравенств или строки коэффициентов целевой функции. В [1] доказано, что гипотеза верна для случая, когда (транспонированная) матрица задачи — это матрица инцидентности графа, а расширенная матрица получается добавлением к ней столбца из единиц. Это соответствует обычной задаче о независимом множестве (все веса равны 1). Здесь доказывается, что это верно и для произвольного вектора весов, т. е. что задача ВНМ решается за полиномиальное время, если миноры матрицы инцидентности с добавленным столбцом весов не превосходят по абсолютной величине некоторой константы.

Для дерева T и вектора весов $w = (w_1, w_2, ...w_n)$ обозначим через $D(T, w)$ абсолютную величину определителя матрицы, получающейся добавлением столбца w к матрице инцидентности дерева. Следующая лемма доказывается аналогично лемме 2 из работы [1].

Лемма 1. *Пусть W_1 и W_2 — суммы весов вершин в долях двудольного разложения дерева T. Тогда $D(T, w) = |W_1 - W_2|$.*

Для графа G и вектора весов w обозначим через $M(G, w)$ максимум абсолютных величин миноров матрицы, получаемой добавлением столбца w к матрице инцидентности этого графа.

Лемма 2. *Если T — дерево с не менее чем k листьями, то $M(T, w) \geq k/4$ для любого w.*

Доказательство. Пусть W_1 и W_2 — суммы весов вершин в долях двудольного разложения дерева T, причем $W_1 \geq W_2$. Тогда $D(T, w) = W_1 - W_2$. Допустим,что $W_1 - W_2 < k/4$.

Рассмотрим дерево T', получающееся из дерева T удалением всех листьев из той доли, где их не меньше половины. Пусть w' — соответствующий вектор весов, W_1',W_2' — суммарные веса долей в T'. Рассмотрим обе возможности.

1. В первой доле не менее $k/2$ листьев. Так как вес каждой вершины не меньше 1, то в этом случае $W_1' \leq W_1 - k/2 < W_2 + k/4 - k/2 = W_2 - k/4 < W_2 = W_2'$. Значит, $D(T', w') = W_2' - W_1' > k/4$.

2. Вторая доля содержит не менее половины листьев. Тогда $W_1' = W_2'$,$W_2' \leq W_2 - k/2$ и $D(T', w') = W_1' - W_2' \geq W_1 - W_2 + k/2 \geq k/2$. Итак, если $D(T/w) < k/4$, то в дереве имеется поддерево T' с $D(T', w') > k/4$. Лемма доказана.

Определим *репей* как граф, получающийся добавлением к нечетному циклу нескольких вершин степени 1 (*шипов*), каждая из кото-

рых соединяется ребром с вершиной цикла, причем каждая вершина цикла смежна не более чем с одним шипом. Графы, не имеющие общих вершин, называем *разобщенными*. Обозначим через $B_{p,q}$ класс всех графов, не содержащих p разобщенных нечетных циклов и репьев с q шипами.

Лемма 3. *Если* $M(G,w) \le k$, *то* $G \in B_{\lfloor \log_2 k \rfloor + 1, 4k+4}$.

Доказательство. Известно [4], что максимальная абсолютная величина минора матрицы инцидентности графа равна 2^t, где t — наибольшее число разобщенных нечетных циклов в графе. Значит, если $M(G,w) \le k$, то $2^t \le k$ и в графе имеется не более чем $\lfloor \log_2 k \rfloor$ разобщенных нечетных циклов. Если в графе имеется репей с $4k+4$ шипами, то удалением любого ребра из содержащегося в нем цикла этот репей превращается в дерево с не менее чем $4k+4$ листьями. Тогда, по лемме 2, $M(G,w) \ge k+1$. Лемма доказана.

Теорема 1. *Для любых* p *и* q *существует алгоритм, решающий за полиномиальное время задачу ВНМ для любого графа* $G \in B_{p,q}$ *и любого вектора весов* w.

Доказательство этой теоремы почти дословно повторяет доказательство теоремы 6 из работы [1], утверждающей, что задача о независимом множестве (с единичными весами) решается за полиномиальное время для графов из класса $B_{p,q}$ при любых фиксированных p и q. Единственное необходимое уточнение связано с тем, что в доказательстве из [1] используется полиномиальная разрешимость задачи о независимом множестве для двудольных графов (хорошо известный факт) и для простых циклов (очевидная). Для задачи с произвольными весами оба утверждения также справедливы (см., например, [3]).

Из теоремы 1 и леммы 3 следует

Теорема 2. *Для любого* k *существует алгоритм, решающий за полиномиальное время задачу ВНМ для любого графа* G *и любого вектора весов* w *таких, что* $M(G,w) \le k$.

Список литературы

1. Алексеев В. Е., Захарова Д. В. Независимые множества в графах с ограниченными минорами расширенной матрицы инцидентности // Дискретный анализ и исследование операций. — 2010. — Т. 17. — С. 3–10.

2. Шевченко В. Н. Качественные вопросы целочисленного программирования. — М.: Наука, 1995.

3. Alekseev V. E., Lozin V. V. Independent sets of maximum weight in (p,q)-colorable graphs // Discrete Mathematics. — 2003. — V. 265. — P. 351–356.

4. Grossman J. W., Kilkarni D. M., Schochetman I. E. On the minors of an incidence matrix and its Smith normal form // Linear Algebra and its Applications. — 1995. — V. 218. — P. 213–224.

КОНСТРУКТИВНЫЕ ОПИСАНИЯ РАСЩЕПЛЯЕМЫХ ГРАФОВ

М. А. Иорданский (Нижний Новгород)

Рассматриваются обыкновенные неориентированные графы. Используются следующие обозначения: $V(G)$ — множество вершин графа G; $G(V')$ — подграф графа G, порожденный подмножеством вершин $V' \in V$; K_n — полный n-вершинный граф (K_0 — граф, не содержащий вершин); $\overline{G}$ — дополнение графа G до полного.

В работе используется конструктивный подход к представлению графов [1]. На множестве графов $\Im$ рассматриваются отображения $\Im \times \Im \longrightarrow \Im$, в которых результирующий граф отображения G допускает представление в виде объединения с пересечением подграфов, изоморфных исходным графам G_1 и G_2. Эти отображения интерпретируются как *операции склейки* графов-операндов G_1 и G_2 по подграфам $G_1' \subseteq G_1$ и $G_2' \subseteq G_2$, изоморфным *подграфу склейки* $\tilde{G} \subseteq G$. Операция склейки называется *тривиальной*, если $G_1' = G_1$ и (или) $G_2' = G_2$. Тривиальные операции склейки не позволяют получать новых графов и поэтому далее не рассматриваются. Тот факт, что граф G получен в результате выполнения операции склейки графов G_1 и G_2 по подграфам, изоморфным $\tilde{G}$, обозначается следующим образом $G \Leftarrow (G_1 \circ G_2)\,\tilde{G}$. Граф G может зависеть в общем случае также от выбора подграфов $G_1' \subseteq G_1$ и $G_2' \subseteq G_2$, изоморфных $\tilde{G}$, и способа их отождествления. Операции склейки с изоморфными подграфами $\tilde{G}$ относятся к одному *типу*.

Пусть все графы из $\Im$ обладают заданным характеристическим свойством; H — система ограничений на операции склейки, обеспечивающая сохранение характеристического свойства графов. Операции, удовлетворяющие системе ограничений H, называются для краткости операциями *H-склейки*. Граф G называется *H-суперпозицией* графов из $\Im$, если $G \in \Im$ или G можно получить из графов множества $\Im$ путем последовательного применения операций H-склейки. Процессу построения графа G соответствует *операция*

H-суперпозиции графов из $\Im$. $[\Im]_H$ — множество всех графов, получаемых из $\Im$ с помощью операций H-суперпозиции. Класс графов $\Im$ называется *H-замкнутым*, если $[\Im]_H = \Im$. Минимальное по включению подмножество графов $\Im' \subset \Im$, достаточное для получения всех графов H-замкнутого класса $\Im$ с помощью операций H-суперпозиции, образует его *элементный базис* B_e. Операция H-суперпозиции называется *канонической*, если один из графов-операндов каждой операции H-склейки изоморфен некоторому графу из B_e. Минимальное по включению множество операций H-склейки различных типов, достаточное для построения исходя из графов B_e всех графов H-замкнутого класса $\Im$, образует его *операционный базис* B_o. Операционный базис задается множеством соответствующих подграфов склейки. *Конструктивное описание* H-замкнутого класса $\Im$ определяется тройкой $< H, B_e, B_o >$. H-замкнутый класс $\Im$ имеет *конечное описание*, если множества B_e и B_o содержат конечное число графов.

Граф G называется *расщепляемым*, если существует разбиение $V(G) = V_1 \cup V_2$ такое, что подграф $G(V_1)$ является полным, а $G(V_2)$ — пустым. Множество V_1 или V_2 может быть пустым. Нетрудно видеть, что если расщепляемый граф не является связным, то все его компоненты связности, кроме быть может одной, являются изолированными вершинами. Справедлива

Лемма. *В расщепляемом связном графе* G, $|V(G)| = n, n \geq 3$, *не являющемся полным, найдется максимальный полный подграф* G_0 *такой, что* $|V(G_0) \cap V(G_i)| = |V(G_i)| - 1$, $1 \leq i \leq l$, $l \leq n-2$, *где* G_i, $i = \overline{1,l}$, *все другие максимальные полные подграфы графа* G.

Подграф G_0 называется *опорным*. В общем случае в графе G можно выделить несколько опорных подграфов G_0. Входящие в них вершины будем называть *потенциально опорными*. Каждый подграф G_0 является одним из наибольших полных подграфов в G. Для упрощения изложения полный граф G также считается опорным.

Из леммы следует, что расщепляемый граф G можно рассматривать как результат операции H-суперпозиции графов G_i, $i = \overline{0,l}$, со структурой $(\ldots(G_0 \circ G_1)\tilde{G}_1 \circ G_2)\tilde{G}_2 \circ \ldots \circ G_l)\tilde{G}_l$, где все операции склейки производятся по полным подграфам, принадлежащим G_0 в графе-операнде, содержащем выбранный опорный подграф. Число вершин в подграфах склейки удовлетворяет равенствам $|V(\tilde{G}_i)| = |V(G_i)| - 1$, $i = \overline{1,l}$. Обозначим эту систему ограничений на операции склейки через $< H_1 >$. Справедлива

Теорема 1. *Класс расщепляемых графов канонически* $< H_1 >$*-замкнут с элементным базисом* $B_e = \{K_1, K_2, \ldots\}$ *и операционным*

базисом $B_o = \{K_0, K_1, \ldots\}$.

При использовании операций склейки по непорожденным подграфам получается конечное описание класса расщепляемых графов. Класс всех обыкновенных графов $\prec H \succ$-замкнут с элементным базисом $B_e = \{K_1, K_2\}$ и операционным базисом $B_o = \{K_0, \overline{K}_2\}$ [1]. В операциях $\prec H \succ$-склейки, каждой паре вершин, несмежных $\tilde{G}$, соответствует пара несмежных вершин хотя бы в одном из графов-операндов. Для сохранения свойства расщепляемости на операции $\prec H \succ$-склейки с текущим (исходным) расщепляемым графом G накладываются следующие ограничения:

1. При склейке графа G с K_2 по $\tilde{G} = K_1$ вершина подграфа K_1 в G должна быть потенциально опорной.

2. При склейке графа G с K_2 по $\tilde{G} = \overline{K}_2$ хотя бы одна из вершин подграфа $\overline{K}_2$ в G должна быть потенциально опорной.

Обозначим указанную систему ограничений на операции склейки через $\prec H_2 \succ$.

Теорема 2. *Класс расщепляемых графов канонически* $\prec H_2 \succ$*-замкнут с элементным базисом* $B_e = \{K_1, K_2\}$ *и операционным базисом* $B_o = \{K_0, \overline{K}_2\}$.

Теорема 3. *Класс связных расщепляемых графов канонически* $\prec H_2 \succ$*-замкнут с элементным базисом* $B_e = \{K_1, K_2\}$ *и операционным базисом* $B_o = \{K_1, \overline{K}_2\}$.

Список литературы

1. Иорданский М. А. Конструктивные описания графов // Дискретный анализ и исследование операций. — 1996. — Т. 3, № 4. — С. 35–63.

О ПОНЯТИИ ГОМОМОРФИЗМА ГРАФОВ

И. Б. Кожухов, В. А. Ярошевич (Москва)

Определение гомоморфизма графов X и Y допускает несколько неэквивалентных друг другу модификаций. В каждом из этих определений гомоморфизмом графов X и Y называется отображение $\alpha : X \to Y$ множеств вершин этих графов, удовлетворяющее определённым условиям, а эндоморфизм графа X — это гомоморфизм $X \to X$. В работе [1] была проведена классификация различных понятий гомоморфизма графа (неориентированного) и изучены

свойства этих отображений. В настоящей работе мы распространяем эти понятия на ориентированные графы и получаем удобную характеризацию гомоморфизмов в терминах бинарных отношений или, что то же самое, булевых матриц и алгебраических операций над ними. Ряд результатов этой работы был опубликован одним из авторов в [2].

Мы будем рассматривать ориентированные графы без кратных рёбер, но допускать наличие петель. Заметим, что задание графа с множеством вершин X равносильно заданию на множестве X бинарного отношения. Как обычно, бинарное отношение σ на множестве X — это подмножество множества $X \times X$. Кроме того, мы будем рассматривать бинарные отношения $\alpha \subseteq X \times Y$, связывающие элементы разных множеств. Умножение бинарных отношений (на одном или разных множествах) определяется обычным образом. Отображения $\alpha : X \to X$, $\beta : X \to Y$ мы будем рассматривать как бинарные отношения. Умножение отображений $\alpha : X \to Y$ и $\beta : Y \to Z$ осуществляется слева направо $x(\alpha\beta) = (x\alpha)\beta$ при $x \in X$. Через $\bar{\sigma}$ мы будем обозначать противоположное отношение: $(a, b) \in \bar{\sigma} \Leftrightarrow (a, b) \notin \sigma$, а через σ^{-1} — обратное отношение: $(a, b) \in \sigma^{-1} \Leftrightarrow (b, a) \in \sigma$.

Приведём теперь соответствующие определения гомоморфизмов графов. Пусть X, Y — произвольные множества, а σ и τ — бинарные отношения на X и на Y соответственно.

Отображение $\alpha : X \to Y$ называется (*обычным*) *гомоморфизмом*, если из $(a, b) \in \sigma$ следует, что $(a\alpha, b\alpha) \in \tau$. Множество всех гомоморфизмов $\alpha : X \to Y$ обозначим $\mathrm{Hom}\,(X, Y)$.

Гомоморфизм $\alpha : X \to Y$ называется *полустрогим*, если из $(a\alpha, b\alpha) \in \tau$ следует, что существуют такие $\bar{a} \in a\alpha\alpha^{-1}$, $\bar{b} \in b\alpha\alpha^{-1}$, что $(\bar{a}, \bar{b}) \in \sigma$. Множество всех полустрогих гомоморфизмов $\alpha : X \to Y$ обозначим $\mathrm{HHom}\,(X, Y)$.

Гомоморфизм $\alpha : X \to Y$ называется *локально строгим*, если из $(a\alpha, b\alpha) \in \tau$ следует, что для каждого $\bar{a} \in a\alpha\alpha^{-1}$ найдётся такое $\bar{b} \in b\alpha\alpha^{-1}$, что $(\bar{a}, \bar{b}) \in \sigma$. Множество всех локально строгих гомоморфизмов $\alpha : X \to Y$ обозначим $\mathrm{LHom}\,(X, Y)$.

Гомоморфизм $\alpha : X \to Y$ называется *квазистрогим*, если из $(a\alpha, b\alpha) \in \tau$ следует, что существует такое $\bar{a} \in a\alpha\alpha^{-1}$, что для каждого $\bar{b} \in b\alpha\alpha^{-1}$ имеет место соотношение $(\bar{a}, \bar{b}) \in \sigma$ и существует такое $\widehat{b} \in b\alpha\alpha^{-1}$, что для каждого $\widehat{a} \in a\alpha\alpha^{-1}$ имеет место соотношение $(\widehat{a}, \widehat{b}) \in \sigma$. Множество всех квазистрогих гомоморфизмов $\alpha : X \to Y$ обозначим $\mathrm{QHom}\,(X, Y)$.

Гомоморфизм $\alpha : X \to Y$ называется *строгим*, если из $(a\alpha, b\alpha) \in$

τ следует, что $(a,b) \in \sigma$. Множество всех строгих гомоморфизмов $\alpha : X \to Y$ обозначим через $\mathrm{SHom}\,(X,Y)$.

Замечание. *В работе* [1] *графы предполагались неориентированными, но, как отмечали сами авторы, определения разных модификаций гомоморфизмов можно использовать для ориентированных графов, что мы и будем делать.*

Оказывается, что рассмотренные в [1] модификации понятия гомоморфизма графа могут быть записаны в компактной форме на языке бинарных отношений.

Теорема. *Пусть* $\alpha : X \to Y$ *— отображение, тогда:*

(i) $\alpha \in \mathrm{Hom}\,(X,Y) \Leftrightarrow \sigma\alpha \subseteq \alpha\tau$;

(ii) $\alpha \in \mathrm{HHom}\,(X,Y) \Leftrightarrow \sigma\alpha \subseteq \alpha\tau \;\&\; \tau \cap (\mathrm{im}\,\alpha \times \mathrm{im}\,\alpha) \subseteq \alpha^{-1}\sigma\alpha$;

(iii) $\alpha \in \mathrm{LHom}\,(X,Y) \Leftrightarrow \sigma\alpha \subseteq \alpha\tau \;\&\; \alpha\tau \cap (X \times \mathrm{im}\,\alpha) \subseteq \sigma\alpha$;

(iv) $\alpha \in \mathrm{QHom}\,(X,Y) \Leftrightarrow \sigma\alpha \subseteq \alpha\tau \;\&\; \alpha(\tau \cap Y \times \mathrm{im}\alpha) \cup \alpha(\tau^{-1} \cap Y \times \mathrm{im}\alpha) \subseteq \alpha\alpha^{-1}\overline{\sigma}\alpha$;

(v) $\alpha \in \mathrm{SHom}\,(X,Y) \Leftrightarrow \sigma\alpha \subseteq \alpha\tau \;\&\; \alpha\tau\alpha^{-1} \subseteq \sigma$.

Если $X = Y$, то мы получаем соответствующие определения эндоморфизмов графов. При этом $\mathrm{End}\,X$ и $\mathrm{SEnd}\,X$ являются моноидами.

Список литературы

1. Bötcher M., Knauer U. Endomorphism spectra of graphs // Discrete Mathematics. — 1992. — V. 109. — P. 45–57. (Postscript: Discrete Mathematics. — 2003. — V. 270. — P. 329–331.)

2. Ярошевич В. А. Отображения, согласующиеся с бинарными отношениями // Математический вестник педвузов и университетов Волго-Вятского региона. — 2009. — Вып. 11. — С. 135–142.

ДВА ЧАСТИЧНЫХ ПАРОСОЧЕТАНИЯ В ДВУДОЛЬНОМ ГРАФЕ СПЕЦИАЛЬНОГО ВИДА

А. М. Магомедов (Махачкала)

В связи с рассмотрением задачи обслуживания *с нефиксированными маршрутами* [1] получено следствие известной теоремы Холла об условиях существования полного паросочетания в двудольном графе [2, 8.13], востребованное в задачах оптимизации расписаний.

Определение. Под реберной 2-раскраской графа в цвета $+1$ и -1 понимается любая раскраска ребер, где каждое ребро раскрашено в один из двух цветов: $+1$ или -1. Количество ребер, инцидентных вершине v и раскрашенных в цвет $+1$ (-1), будем обозначать $\lambda_G^+(v)$ $(\lambda_G^-(v))$. Реберную 2-раскраску графа G будем называть *стационарной* или *уравновешенной* в вершине v, если соответственно

$$\lambda_G^+(v) \cdot \lambda_G^-(v) = 0 \quad \text{или} \quad |\lambda_G^+(v) - \lambda_G^-(v)| \leqslant 1.$$

В следующей теореме через $\Gamma(S)$ обозначено множество вершин, смежных в двудольном графе $G = (X, Y, E)$ вершинам множества $S \subseteq X$.

Теорема. *Пусть простой двудольный граф $G = (X, Y, E)$ удовлетворяет условиям:*

$$|S| \leqslant 2\,|\Gamma(S)| \ \text{ для любого } S \subseteq X; \tag{1}$$

$$d_G x = 2 \ \text{ для каждого } x \in X; \quad d_G y \leqslant 5 \ \text{ для каждого } y \in Y. \tag{2}$$

Тогда существуют подграф $G' = (X, Y', E')$ графа G, включающий множество X, и реберная 2-раскраска графа G, такие, что:

(а) $d_{G'} x = 1$ *для каждого* $x \in X$; $d_{G'} y \leqslant 2$ *для каждого* $y \in Y'$; *если* $d_G y \geqslant 4$, *то* $d_{G'} y = 2$;

(б) *раскраска уравновешена в каждой вершине Y и стационарна в каждой вершине X;*

(в) *если среди ребер, инцидентных какой-либо вершине Y, содержатся два ребра множества E', то цвета этих двух ребер различны.*

Первая часть утверждения теоремы (существование подграфа $G' = (X, Y', E')$, удовлетворяющего условию (а)), означает, что при выполнении условий (1) и (2) множество вершин X допускает разбиение на два таких подмножества X_i, что в подграфе $G_i = (X_i, Y_i, E_i)$ графа G, порожденном на множестве вершин X_i, существует полное паросочетание множества X_i в множество Y_i (*частичное паросочетание* множества X в множество Y); $i = 1, 2$.

Работа выполнена при финансовой поддержке РФФИ, проект 0901-96504-р-юг-а.

Список литературы

1. Танаев В. С., Сотсков Ю. Н., Струсевич В. А. Теория расписаний. Многостадийные системы. — М.: Наука, 1989.

2. Свами М., Тхуласираман К. Графы, сети и алгоритмы. — М.: Мир, 1984.

ПОЧТИ-ИНТЕРВАЛЬНАЯ РЕБЕРНАЯ 6-РАСКРАСКА (3,6)-БИРЕГУЛЯРНОГО ДВУДОЛЬНОГО ГРАФА

А. М. Магомедов, Т. А. Магомедов (Махачкала)

Связи задач реберной раскраски графов с задачами оптимизации расписаний исследованы в работах С. В. Севастьянова, А. С. Астратяна, C. J. Casselgren, Р. Р. Камаляна, В. Г. Визинга, А. В. Пяткина и других авторов.

Пусть задан $(3,6)$-бирегулярный двудольный граф $G = (X, Y, E)$, $|X| = 2n, |Y| = n$.

Задача 1. Существует ли для G интервальная реберная 6-раскраска?

Задача 2. Существует ли для G такая реберная 2-раскраска, что среди ребер, инцидентных каждой вершине из Y, имеется по три ребра каждого цвета, а для каждой вершины из X все три инцидентных ребра одного цвета?

Задача 3 (о непрерывном расписании). Пусть расписание задано в виде $(2n \times 6)$-матрицы, содержащей в каждом столбце n нулевых элементов и множество $N = \{1, \ldots, n\}$, а в каждой строке — точно три элемента из N (необязательно различных). Можно ли привести расписание к *непрерывному виду*, где в каждой строке ненулевые элементы располагаются в подряд идущих ячейках и при этом сохраняются наборы элементов в каждой строке и в каждом столбце?

В [1] доказана NP-полнота задачи 1. NP-полнота задачи о непрерывном расписании в общем виде доказана в [2]. Некоторые аспекты задачи 1 рассмотрены в [3], где доказана эквивалентность задач 1, 2 и 3. Заметим, что если допускаются кратные ребра, то можно построить компактные (с небольшим числом вершин) примеры графа G, для которого ответ на вопрос задачи 1 отрицателен. В случае же обыкновенного графа соответствующие примеры (известные авторам) несколько громоздки; один из них приведен в [4]. В [5] построен метод динамического программирования, отвечающий на вопрос задачи 3.

Определение. Пусть задана реберная 6-раскраска $(3,6)$-бирегулярного двудольного графа $G=(X,Y,E)$, $|X|=2n, |Y|=n$, такая, что среди номеров цветов ребер, инцидентных каждой вершине Y, встречается каждый элемент множества $\{1,2,3,4,5,6\}$ и для каждого $i=1,\ldots,2n$ выполняется неравенство: $c_{\max,i}-c_{\min,i}\leqslant 3$, где $c_{\min,i}$ — наибольший, а $c_{\max,i}$ — наименьший в списке номеров цветов ребер, инцидентных вершине x_i (другими словами, в списке отсутствует разве лишь один элемент интервала $[c_{\min,i},c_{\max,i}]$). Раскраску будем называть *почти-интервальной*, если $\sum_{i=1}^{2n}(c_{\max,i}-c_{\min,i})\leqslant n$.

Задача 4 (о почти-интервальной 6-раскраске). Существует ли почти-интервальная реберная 6-раскраска заданного $(3,6)$-бирегулярного двудольного графа $G=(X,Y,E)$?

Пусть s_i — набор номеров вершин из Y, инцидентных вершине $x_i\in X$, $S=\{s_i\}$; $i=1,\ldots,2n$. С использованием потоковых методов легко проверить возможность выбора из каждого s_i по одному элементу таким образом, чтобы получить *семейство представителей* S_0, включающее каждый элемент интервала $[1,n]$ в точности два раза.

Теорема. *Существование множества представителей S_0 необходимо для положительного ответа на вопрос задачи* 1 *и достаточно для положительного ответа на вопрос задачи* 4.

Работа выполнена при финансовой поддержке РФФИ, проект 0901-96504-р-юг-а.

Список литературы

1. Asratian A. S., Casselgren C. J. Some results on interval edge colorings of (α,β)-biregular bipartite graphs. — Department of Mathematics, Linköping University, Linköping, Sweden, 2008. — S-581 83.

2. Севастьянов С. В. Об интервальной раскрашиваемости ребер двудольного графа // Методы дискретного анализа. Т. 50. — 1990. — С. 61–72.

3. Магомедов А. М. К вопросу об условиях уплотнения матрицы из 6 столбцов. — Деп. в ВИНИТИ, 1991.

4. Магомедов А. М. К вопросу о реберной раскраске двудольного графа // Дискретная математика. — 2009. — Т. 21, вып. 2. — С. 153–159.

5. Магомедов А. М. Уплотнение расписания с директивным сроком, кратным количеству занятий каждого преподавателя // Математические заметки. — 2009. — Т. 85, вып. 1. — С. 65–72.

О ТУПИКОВЫХ ПО ВЫЧИСЛИТЕЛЬНОЙ СЛОЖНОСТИ НАСЛЕДСТВЕННЫХ КЛАССАХ ГРАФОВ

Д. С. Малышев (Нижний Новгород)

К настоящему времени накоплено огромное количество результатов о полиномиальной разрешимости и NP-полноте различных задач на графах во многих классах графов. Способы получения новых сведений такого рода могут быть самими разнообразными, но можно выделить два распространенных подхода:

1. Поиск более широких «простых» классов, объемлющих ранее известные.
2. Поиск NP-полных сужений для известных «сложных» случаев.

Вместе с тем, при рассмотрении представительных семейств классов графов можно ставить задачи более общего характера, чем анализ сложности для индивидуального класса. В частности, можно поставить целью выявление пределов, до которых возможны расширения полиномиальной сложности и сужения с «противоположным» сложностным статусом. Тем самым, речь фактически идет о нахождении границы между «простыми» и «сложными» классами из рассматриваемого семейства. В данной публикации исследуется эта граница для некоторых задач на графах в семействе *наследственных классов графов*, т. е. классов графов, замкнутых относительно удаления вершин.

Формализуем понятия «простого» и «сложного» класса графов. Пусть Π — какая-либо NP-полная задача на графах. Наследственный класс графов назовем Π-*простым*, если задача Π для графов из этого класса полиномиально разрешима, и Π-*сложным* в противном случае. Далее везде предполагаем справедливость неравенства $\mathrm{P}\neq\mathrm{NP}$ и не включаем его явно в формулировки полученных результатов.

Естественной идеей решения задачи демаркации является поиск *максимальных* Π-*простых* и *минимальных* Π-*сложных классов*, т. е. тупиковых классов графов соответствующей сложности из рассматриваемой решетки. К сожалению, использование понятия максимального простого класса графов оказывается безрезультатным. Так, В. Е. Алексеев в работе [1] установил, что ни один простой для задачи о независимом множестве класс не является максимальным простым. Однако, рассуждения из данной работы легко переносятся на случай произвольной задачи на графах, таким образом, максимальных простых классов нет ни для одной задачи. Вместе с тем, до недавнего времени про минимальные сложные классы ничего не было известно.

Первый результат о подобного рода классах был получен автором в работе [2]. Там рассматривалась задача распознавания при-

надлежности наследственному классу графов $\mathbf{X}$ (задача РП[$\mathbf{X}$]) и было доказано следующее утверждение.

Теорема 1. *Для любого класса графов* $\mathbf{X}$ *ни один* РП[$\mathbf{X}$]*-сложный класс графов не является минимальным* РП[$\mathbf{X}$]*-сложным.*

Поскольку классические NP-полные при $k > 2$ задачи о вершинной k-раскраске и о реберной k-раскраске являются переформулировками задачи распознавания принадлежности наследственному классу графов, то они — примеры задач, для которых нет минимальных сложных классов.

В той же работе [2] были найдены минимальные сложные классы графов для некоторых модификаций классических задач о раскраске. Речь идет о задачах о списковом ранжировании, сформулированных в работах [3] и [4]. Постановка задачи о вершинном списковом ранжировании (задачи ВСР) состоит в следующем. Пусть заданы граф G с множеством вершин V и множество $\mathcal{L} = \{L(v) : \ v \in V\}$, где каждое $L(v)$ — конечное множество натуральных чисел. *$\mathcal{L}$-ранжированием* графа G называется такая раскраска c его вершин, что:

1) $c(v) \in L(v)$ для каждой вершины v;

2) если $c(u) = c(v)$, $u \neq v$, то каждый путь, соединяющий u и v, содержит такую вершину w, что $c(w) > c(u)$.

Задача ВСР состоит в том, чтобы по данным G и $\mathcal{L}$ определить, существует ли $\mathcal{L}$-ранжирование графа G. В задаче РСР о реберном ранжировании списки допустимых цветов назначаются ребрам и ищется реберная раскраска, удовлетворяющая вышеприведенным требованиям, в которых слово «вершина» заменено словом «ребро».

Необходимо уточнить, что под ВСР (РСР)-простым классом графов далее понимается такой наследственный класс, что соответствующая задача решается для графов из этого класса за полиномиальное время при любом множестве $\mathcal{L}$.

В работе [2] рассматривались *кометы*, т. е. графы, получаемые отождествлением центральной вершины звезды с одной из концевых вершин простого пути. Класс `Comet` — наследственное замыкание множества комет, а класс `Hammer` — наследственное замыкание реберных графов к графам из `Comet`. Значение этих двух классов графов раскрывает следующий результат работы [2].

Теорема 2. *Класс* `Comet` *является минимальным* ВСР*-сложным и минимальным* РСР*-сложным, а класс* `Hammer` *является минимальным* ВСР*-сложным.*

Обозначим через `Star` наследственное замыкание множества деревьев высоты два, имеющих ровно одну вершину степени не менее чем 3 — корень. Пусть `Sun` — наследственное замыкание множества графов, являющихся реберными к графам из `Star`. Для этих двух классов имеет место следующее утверждение, подобное теореме 2.

Теорема 3. *Класс* Star *является минимальным* BCP*-сложным и минимальным* PCP*-сложным, а класс* Sun *является минимальным* BCP*-сложным.*

Важное различие между множествами классов $\{\texttt{Comet}, \texttt{Hammer}\}$ и $\{\texttt{Star}, \texttt{Sun}\}$ состоит в том, что второе множество составляют классы, задаваемые конечным множеством запрещенных порожденных подграфов.

Список литературы

1. Alekseev V. E. On easy and hard hereditary classes of graphs with respect to the independent set problem // Discrete Applied Mathematics. — 2004. — V. 132. — P. 17–26.

2. Малышев Д. С. О минимальных сложных классах графов // Дискретный анализ и исследование операций. — 2009. — Т. 16, № 6. — С. 23–31.

3. Jamison R. E. Coloring parameters associated with rankings of graphs // Congressus Numerantum. — 2003. — V. 164. — P. 111–127.

4. Dereniowski D. The complexity of list ranking of trees // Ars Combinatoria. — 2008. — V. 86. — P. 97–114.

АЛГОРИТМ ПРИБЛИЖЕННОГО РЕШЕНИЯ ЗАДАЧИ АППРОКСИМАЦИИ ГРАФА

А. А. Навроцкая (Омск)

В настоящей работе доказаны априорная и апостериорная оценки погрешности приближенного алгоритма для задачи аппроксимации графа, когда число компонент аппроксимирующего графа произвольно.

M-графом называется обыкновенный граф, т. е. без петель и кратных ребер, каждая компонента связности которого есть полный граф. Класс всех M-графов на множестве вершин V обозначим $\mathcal{M}(V)$.

Пусть $G_1 = (V, E_1)$ и $G_2 = (V, E_2)$ — помеченные графы, тогда *расстояние* между данными графами определяется следующим образом: $\rho(G_1, G_2) = |E_1 \triangle E_2|$, где $E_1 \triangle E_2 = (E_1 \setminus E_2) \cup (E_2 \setminus E_1)$.

Через $D(G_1, G_2)$ обозначим граф на множестве вершин V с множеством ребер $E_1 \triangle E_2$. Число ребер в графе $D(G_1, G_2)$ равно расстоянию $\rho(G_1, G_2)$.

Задача аппроксимации графа. Дан обыкновенный n-вершинный граф $G = (V, E)$. Найти граф $M^* \in \mathcal{M}(V)$ такой, что

$$\rho(G, M^*) = \min_{M \in \mathcal{M}(V)} \rho(G, M).$$

В [1] доказано, что задача аппроксимации графа NP-трудна, следовательно актуальным направлением является разработка алгоритмов приближенного решения этой задачи.

Лемма. *Пусть* $D = D(G_1, G_2)$, $d_{\min}$ — *минимум степеней вершин в графе* D, $n = |V|$. *Тогда*

$$\rho(G_1, G_2) \geq \frac{n d_{\min}}{2}.$$

Через $N_G(v)$ обозначим множество смежных с v вершин в графе G, а $\overline{N_G(v)} = V \setminus (N_G(v) \cup \{v\})$. Пусть величина $\tilde{\rho}(v, G)$ равна сумме числа отсутствующих ребер в подграфе графа G, порожденном множеством вершин $N_G(v) \cup \{v\}$, и величины разреза $(N_G(v) \cup \{v\}, V \setminus N_G(v) \cup \{v\})$ в графе G.

Для приближенного решения поставленной задачи предложен следующий алгоритм.

`Алгоритм` N.

`Шаг` 1. Положим $G_1 = G$. Выберем вершину v_1 такую, что $\tilde{\rho}(v_1, G) = \min \tilde{\rho}(v_j, G)$, где минимум берется по всем $v_j \in V$. Положим $V_1 = N_{G_1}(v_1) \cup \{v_1\}$. Если $V \setminus V_1 = \emptyset$, то стоп. Иначе переходим на шаг 2.

`Шаг` $i, i \geq 2$. Обозначим через G_i подграф графа G_{i-1}, порожденный множеством вершин $V \setminus (V_1 \cup V_2 \cup ... \cup V_{i-1})$. Пусть вершина v_i такая, что $\tilde{\rho}(v_i, G_i) = \min \tilde{\rho}(v_j, G_i)$, где минимум берется по всем $v_j \in V \setminus (V_1 \cup V_2 \cup ... \cup V_{i-1})$. Положим $V_i = N_{G_i}(v_i) \cup \{v_i\}$. Если $V \setminus (V_1 \cup ... \cup V_i) = \emptyset$, то стоп. Иначе переходим на шаг $i + 1$.

`Конец.`

Пусть l — число построенных множеств V_i $(1 \leq l \leq n)$. Рассмотрим M-граф $M_N = M(V_1, V_2, ..., V_l) \in \mathcal{M}$, где $M(V_1, V_2, ..., V_l)$ — M-граф, в котором множество V_i порождает полный подграф, $i \in \{1, ..., l\}$.

Замечание. *Пусть* M_i — *оптимально аппроксимирующий граф из класса* $\mathcal{M}(V \setminus (V_1 \cup V_2 \cup ... \cup V_{i-1}))$ *для графа* G_i, $i \in \{1, ..., l\}$. *Тогда* $\rho(G_1, M_1) \geq \rho(G_i, M_i)$.

Имеет место следующая апостериорная оценка погрешности алгоритма N.

Теорема. *Дан граф G. Пусть M_N — граф найденный алгоритмом N. Тогда*

$$\frac{\rho(G, M_N)}{\rho(G, M^*)} \leq 3l,$$

где M^* — оптимально аппроксимирующий M-граф для G.

Доказательство. Представим $\rho(G, M_N)$ следующим образом:

$$\rho(G, M_N) = \tilde{\rho}(v_1, G_1) + \tilde{\rho}(v_2, G_2) + \ldots + \tilde{\rho}(v_l, G_l).$$

Поделим обе части равенства на $\rho(G, M^*)$.

$$\frac{\rho(G, M_N)}{\rho(G, M^*)} = \frac{\tilde{\rho}(v_1, G_1)}{\rho(G, M^*)} + \frac{\tilde{\rho}(v_2, G_2)}{\rho(G, M^*)} + \ldots + \frac{\tilde{\rho}(v_l, G_l)}{\rho(G, M^*)}.$$

Используя замечание, получаем

$$\frac{\rho(G, M_N)}{\rho(G, M^*)} \leq \frac{\tilde{\rho}(v_1, G_1)}{\rho(G_1, M_1)} + \frac{\tilde{\rho}(v_2, G_2)}{\rho(G_2, M_2)} + \ldots + \frac{\tilde{\rho}(v_l, G_l)}{\rho(G_l, M_l)}. \qquad (1)$$

В процессе работы алгоритма на каждом шаге выбираем минимальное $\tilde{\rho}(v_i, G_i)$, следовательно верно неравенство $\tilde{\rho}(v_i, G_i) \leq \tilde{\rho}(v_i^*, G_i)$, где v_i^* — вершина минимальной степени в графе $D_i = D(G_i, M_i)$ и M_i — оптимально аппроксимирующий граф для G_i. Построим граф $\widetilde{M}_i$, изменив оптимальное решение M_i следующим образом. Все вершины, множества $N_{G_i}(v_i^*) \cap N_{D_i}(v_i^*)$, переместим в компоненту, содержащую v_i^*, а все вершины принадлежащие множеству $\overline{N_{G_i}(v_i^*)} \cap N_{D_i}(v_i^*)$ перенесем из компоненты, содержащей вершину v_i^*, в другие компоненты M-графа. Число перемещений равно d_i — степени вершины v_i^* в графе D_i, а каждое перемещение не может увеличить значение целевой функции более, чем на $n_i - 1$, где n_i — число вершин графа G_i. Полученное решение хуже оптимального не более, чем на $d_i(n_i - 1)$.

$$\tilde{\rho}(v_i, G_i) \leq \tilde{\rho}(v_i^*, G_i) \leq \rho(G_i, \widetilde{M_i}) \leq \rho(G_i, M_i) + d_i(n_i - 1).$$

Тогда с учетом леммы получаем.

$$\frac{\tilde{\rho}(v_i, G_i)}{\rho(G_i, M_i)} \leq \frac{\rho(G_i, M_i) + d_i(n_i - 1)}{\rho(G_i, M_i)} \leq 1 + \frac{2d_i(n_i - 1)}{d_i n_i} \leq 3.$$

Данное неравенство верно для всех слагаемых в (1), следовательно

$$\frac{\rho(G, M_N)}{\rho(G, M^*)} \leq 3l.$$

Теорема доказана.

Следствие. *Для произвольного n-вершинного графа G алгоритм N находит M-граф M_N такой, что*

$$\frac{\rho(G, M_N)}{\rho(G, M^*)} \leq 3n,$$

где M^* — оптимально аппроксимирующий M-граф для графа G.

Список литературы

1. Агеев А. А., Ильев В. П., Кононов А. В., Талевнин А. С. Вычислительная сложность задачи аппроксимации графов // Дискретный анализ и исследование операций. Сер. 1. — 2006. — Т. 13, № 1. — С. 3–15.

О НЕКОТОРЫХ КРИТЕРИЯХ ОЦЕНКИ ПОКРЫТИЙ С УПОРЯДОЧЕННЫМ ОХВАТЫВАНИЕМ

Т. А. Панюкова, Е. А. Савицкий (Челябинск)

Допустим, для задачи раскроя необходимо определить оптимальный ход режущего инструмента при заданном размещении деталей на плоскости. В автоматизированной системе технологической подготовки процессов раскроя листового материала математической моделью раскройного плана является плоский граф. Целью моделирования является определение такой кратчайшей траектории режущего инструмента, чтобы отрезанная от листа часть не требовала дополнительных разрезаний. Формально множество таких траекторий может быть определено как покрытие с упорядоченным охватыванием для плоского графа.

Будем говорить, что последовательность реберно-непересекающихся цепей

$$C^0 = v^0 e_1^0 v_1^0 e_2^0 \ldots e_{k_0}^0 v_{k_0}^0, \quad C^1 = v^1 e_1^1 v_1^1 e_2^1 \ldots e_{k_1}^1 v_{k_1}^1, \ldots,$$

$$C^{n-1} = v^{n-1} e_1^{n-1} v_1^{n-1} e_2^{n-1} \ldots e_{k_{n-1}}^{n-1} v_{k_{n-1}}^{n-1}$$

с упорядоченным охватыванием, покрывающая граф G и такая, что

$$(\forall m:\ m<n)\,,\quad \left(\bigcup_{l=0}^{m-1}\mathrm{Int}(C^l)\right)\cap\left(\bigcup_{l=m}^{n-1}C^l\right)=\emptyset$$

является покрытием с упорядоченным охватыванием [1].

Построение покрытия графа G с упорядоченным охватыванием решает поставленную задачу раскроя. Наибольший интерес представляют покрытия с минимальным числом цепей, поскольку переход от одной цепи к другой соответствует холостому проходу режущего инструмента.

Минимальную по мощности последовательность реберно-непересекающихся цепей с упорядоченным охватыванием в плоском графе G будем называть эйлеровым покрытием с упорядоченным охватыванием.

Доказательство теоремы существования решения конструктивно и состоит в доказательстве результативности алгоритма построения покрытия последовательностью цепей с упорядоченным охватыванием. Теорема существования таких последовательностей цепей и алгоритм их построения приведены в [2].

Пусть для некоторого набора деталей имеется несколько раскройных планов. Требуется найти множество раскройных планов, для которых покрытие цепями с упорядоченным охватыванием было бы оптимальным.

Рассмотрим возможные критерии оптимальности. Стоимость раскроя зависит в основном от трех факторов: длины пути холостого хода, длины пути реза, количества точек врезки [3] и пр.

Количество холостых проходов (*число точек врезки*). Задача их минимизации тривиальна. В данном случае необходимо рассмотреть все имеющиеся упаковки и выбрать те, для которых в соответствующем им плоском графе число вершин нечетной степени будет минимально, и построить покрытия цепями с упорядоченным охватыванием. Такая задача решается за линейное время.

Суммарная длина пути реза. Эта задача также может быть решена за линейное время еще на этапе кодирования графа.

Длина пути холостого хода. Эта задача не так тривиальна. В частности, алгоритм для задачи китайского почтальона не подходит, так как в данном случае при построении маршрута уровень вложенности каждой вершины определяет допустимый порядок обхода. С целью уменьшения длины маршрута можно рекомендовать идти в ближайшую непомеченную вершину $v\in V_{odd}$ с максимальным уровнем вложенности (т. е. жадный алгоритм). Вычислительный эксперимент показывает, что построенный таким образом маршрут

имеет длину не больше маршрута, найденного с помощью алгоритма [1], когда очередная вершина $v \in V_{odd}$ для врезки выбиралась лексикографически.

Заметим, что алгоритм построения покрытия с упорядоченным охватыванием решает поставленную задачу только для односвязного графа. Этот случай типичен для задач прямоугольного раскроя. Однако возможны случаи, когда раскройный план представлен многосвязным графом, например, когда на раскройном листе имеются дефекты. Нетрудно заметить, что в данном случае возможна модификация разработанного алгоритма. Если компоненты связности не являются вложенными, то проблема сведется к задаче построения покрытия для каждой компоненты связности в отдельности. В случае, когда компоненты связности вложены, процедуру "Упорядочение" необходимо погрузить в цикл, чтобы она выполнилась для каждой вложенной компоненты связности. В данном случае основная трудность заключается в распознавании ребер, принадлежащих внешней грани f_0 для вложенных компонент связности (f_0 в данном случае определяется при отсутствии внешних компонент связности). Эта задача может быть решена, например, с помощью волнового алгоритма. Далее можно связать вложенные компоненты связности с помощью введения мостов между ними, а затем выполнить алгоритм построения покрытия для модифицированного графа.

Список литературы

1. Panyukova T. Chain sequences with ordered enclosing // Journal of Computer and System Sciences International. — 2007. — V. 46, № 1; 10. — P. 83–92.

2. Panyukova T. Cover with ordered enclosing for flat graphs. — Electronic Notes in Discrete Mathematics. — 2007. — № 28. — P. 17–24.

3. Верхотуров М. А., Тарасенко П. Ю. Математическое обеспечение задачи оптимизации пути режущего инструмента при плоском фигурном раскрое на основе цепной резки // Вестник УГАТУ. Сер. Управление, вычислительная техника и информатика. — 2008. — Т. 10, № 2 (27). — С. 123–130.

О КВАДРАТНОЙ 1-ФАКТОРИЗАЦИИ n-МЕРНОГО КУБА

А. Я. Петренюк, М. Ф. Семенюта (Кировоград)

Рассмотрим n-мерный (булев) куб Q_n. В работе [1] положено начало перечислениям неизоморфных 1-факторизаций графа Q_n. Под

1-факторизацией графа G понимают множество Φ 1-факторов этого графа, таких, что каждое ребро графа G принадлежит одному и только одному фактору из Φ. 1-Факторизацию графа $G = (V, E)$ называют *совершенной*, если каждое попарное объединение ее 1-факторов является $|V|$-вершинным циклом.

Теорема 1. *Если подстановка α является автоморфизмом 1-факторизации Φ графа Q_n, то число неподвижных элементов в α четное.*

Теорема 2. *Если подстановка α является автоморфизмом 1-факторизации Φ графа Q_n и α имеет больше, чем 2^{n-1} неподвижных элементов, то число неподвижных элементов в α равно 2^n.*

Теорема 3. *Если подстановка α является автоморфизмом 1-факторизации Φ графа Q_n и в α существует 2^{n-1} неподвижных элементов, то остальные 2^{n-1} элемента также неподвижны в α.*

Граф Q_n допускает квадратную 1-факторизацию при каждом n. При $n = 2; 3; 4$ квадратная 1-факторизация единственная [1].

Теорема 4. *Квадратная 1-факторизация графа Q_n единственная с точностью до изоморфизма для каждого n.*

Список литературы

1. Петренюк А. Я. Екстремальні розклади повних графів: існування, перелік. — Дис. д-ра фіз.-мат. наук: 01.05.01. — К., 2002.

О (0,1)-МАТРИЦАХ С РАВНЫМИ ЕДИНИЦЕ ПОЛУПЕРМАНЕНТАМИ

В. Б. Поплавский (Саратов)

Задача сохранения матричных свойств при преобразовании матриц с элементами из некоторого полукольца является одной из самых широко представленных работами по этой теме в современной математической литературе (см., например, обзор [1]). В этой статье изучаются свойства множества квадратных матриц $\mathbf{M}$ над булевой $\{0,1\}$-алгеброй с полуперманентами равными 1, которые для матрицы $A = (a^i_j)$ определяются формулами

$$\overset{+}{\nabla} A = \bigcup_{(\lambda_1,\ldots,\lambda_n)\in \overset{+}{P}} \cap_{k=1}^{n} a_k^{\lambda_k}, \quad \overset{-}{\nabla} A = \bigcup_{(\lambda_1,\ldots,\lambda_n)\in \overset{-}{P}} \cap_{k=1}^{n} a_k^{\lambda_k}.$$

Здесь $\overset{+}{P}$ и $\overset{-}{P}$ обозначают множества всех четных и нечетных n подстановок ($n \geq 2$). Доказывается утверждение о том, что произвольный матричный многочлен с аргументами из $\mathbf{M}$ и коэффициентами из булевой $\{0,1\}$-алгебры сохраняет равенство полуперманентов. Таким образом, мы даем примеры нелинейных преобразований, сохраняющих линейные инварианты бинарных отношений на конечном множестве, каковыми являются полуперманенты $\{0,1\}$-матриц, соответствующих этим бинарным отношениям на конечном множестве. В качестве следствий получаем, что множество $\mathbf{M}$, пополненное нулевой матрицей, является одновременно полукольцом и полумодулем над булевой $\{0,1\}$-алгеброй.

Теорема. *Произвольный матричный многочлен*

$$f(A,B,C,...) = \bigcup_{i=0}^{r_i} \bigcup_{j=0}^{r_j} \bigcup_{k=0}^{r_k} ...(\lambda_{ijk...} \cap A^{m_i} B^{n_j} C^{p_k} ...),$$

с аргументами из множества $\mathbf{M}$ *булевых квадратных* $\{0,1\}$*-матриц одинаковых размеров с полуперманентами равными* 1 *и коэффициентами* $\lambda_{ijk...}$ *из булевой* $\{0,1\}$*-алгебры сохраняет равенство полуперманентов. При этом, если не все коэффициенты* $\lambda_{ijk...}$ *равны нулю, то и* $\overset{+}{\nabla} f(A,B,C,...) = \overset{-}{\nabla} f(A,B,C,...) = 1$.

Доказательство. Следует показать, во-первых, что произведение $A \cdot B$ матриц A, B с полуперманентами равными 1 есть матрица с полуперманентами равными 1. Во-вторых, объединение $A \cup B$ матриц A, B из $\mathbf{M}$ есть матрица из $\mathbf{M}$.

Для доказательства первого воспользуемся известными формулами для полуперманентов (см., например, [2; 3; 4, §19]):

$$(\overset{+}{\nabla} A \cap \overset{+}{\nabla} B) \cup (\overset{-}{\nabla} A \cap \overset{-}{\nabla} B) \subseteq \overset{+}{\nabla} (A \cdot B),$$

$$(\overset{-}{\nabla} A \cap \overset{+}{\nabla} B) \cup (\overset{+}{\nabla} A \cap \overset{-}{\nabla} B) \subseteq \overset{-}{\nabla} (A \cdot B).$$

Следовательно, из $\overset{\pm}{\nabla} A = \overset{\pm}{\nabla} B = 1$ получаем $\overset{\pm}{\nabla} (A \cdot B) = 1$.

Показать, что объединение матриц $A \cup B$ с полуперманентами равными 1 есть матрица с полуперманентами равными 1, можно таким же образом, если учитывать неравенства

$$\overset{+}{\nabla} A \cup \overset{+}{\nabla} B \subseteq \overset{+}{\nabla} (A \cup B), \quad \overset{-}{\nabla} A \cup \overset{-}{\nabla} B \subseteq \overset{-}{\nabla} (A \cup B),$$

которые несложно проверить.

То, что пересечение $\lambda \cap A$ матрицы A с равными полуперманентами с булевым коэффициентом λ есть матрица с равными полуперманентами является совершенно очевидным.

Таким образом, произвольный матричный многочлен с аргументами из $\mathbf{M}$ и коэффициентами из булевой $\{0,1\}$-алгебры сохраняет равенство полуперманентов.

Пример. Нетрудно увидеть, что множество матриц размера 2×2 с равными 1 полуперманентами состоит из одной матрицы вида $A = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$. Матрицами размера 3×3 из $\mathbf{M}$ являются матрицы вида

$$A = \begin{pmatrix} 1 & 1 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \qquad B = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 1 & 1 \end{pmatrix}, \qquad C = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix}$$

и любые матрицы, которые содержат указанные матрицы A или B, или C.

Следствие 1. *Множество $\mathbf{M} \cup \{O\}$ булевых квадратных $\{0,1\}$-матриц одинаковых размеров с полуперманентами равными 1, пополненное нулевой матрицей O, является полукольцом с аддитивной операцией $\cup$ и мультипликативной операцией произведения булевых матриц.*

Доказательство. Достаточно проверить выполнение законов дистрибутивности:

$$(A \cup B) \cdot C = A \cdot C \cup B \cdot C, \qquad A \cdot (B \cup C) = A \cdot B \cup A \cdot C.$$

Действительно, для элемента $((A \cup B) \cdot C)^i_j$, стоящего в строчке i и столбце j матрицы $(A \cup B) \cdot C$ получаем

$$\begin{aligned} ((A \cup B) \cdot C)^i_j &= \bigcup_k ((A^i_k \cup B^i_k) \cap C^k_j) = \\ &= \bigcup_k (A^i_k \cap C^k_j) \cup \bigcup_k (B^i_k \cap C^k_j) = (A \cdot C \cup B \cdot C)^i_j. \end{aligned}$$

Вторая формула доказывается аналогично.

Следствие 2. *Множество $\mathbf{M} \cup \{O\}$ булевых квадратных $\{0,1\}$-матриц одинаковых размеров с полуперманентами равными 1, пополненное нулевой матрицей O, является полумодулем с аддитивной операцией объединения матриц над полукольцом скаляров, которым является булева $\{0,1\}$-алгебра.*

Доказательство. То, что любая линейная комбинация матриц из $\mathbf{M} \cup \{O\}$ является матрицей из $\mathbf{M} \cup \{O\}$, очевидно, является следствием доказанной выше теоремы. Таким образом, $\mathbf{M} \cup \{O\}$ образует полумодуль, то есть непустое множество с двумя операциями,

объединением матриц $A \cup B = (a^i_j \cup b^i_j) \in \mathbf{B}_{m\times n}$ (заменяющим сложение) и пересечением матрицы с элементом из булевой алгебры $\lambda \cap A = (\lambda \cap a^i_j) \in \mathbf{B}_{m\times n}$(заменяющим умножение на скаляр), которые удовлетворяют для любых матриц и булевых скаляров следующим аксиомам: 1. $(A \cup B) \cup C = A \cup (B \cup C)$, 2. $A \cup B = B \cup A$, 3. $A \cup O = A$, 4. $1 \cap A = A$, 5. $(\alpha \cap \beta) \cap A = \alpha \cap (\beta \cap A)$, 6. $(\alpha \cup \beta) \cap A = (\alpha \cap A) \cup (\beta \cap A)$, 7. $\alpha \cap (A \cup B) = (\alpha \cap A) \cup (\alpha \cap B)$.

Список литературы

1. Гутерман А. Э., Михалев А. В. Общая алгебра и линейные отображения, сохраняющие матричные инварианты // Фундаментальная и прикладная математика. — 2003. — Т. 9, № 1. — С. 83–101.

2. Поплавский В. Б. Ориентированные определители произведения булевых матриц // Математика, механика: Сб. науч. тр. Вып. 6. — Саратов: Изд-во Сарат. ун-та, 2004. — С. 111–114.

3. Golan J. S. Semirings and their applications. — Dordrecht: Kluwer Academic Publishers, 1999.

4. Reutenauer C, Straubing H. Inversion of matrices over a commutative semiring // Journal of Algebra. — 1984. — V. 88. — P. 350–360.

ОБ ОПРЕДЕЛЕНИЯХ ГОМОМОРФИЗМА ГИПЕРГРАФОВ

А. В. Решетников (Москва)

Различные виды гомоморфизмов графов были подробно рассмотрены в работе [1]. В работе [2] определения были обобщены на случай произвольных бинарных отношений следующим образом. Пусть на множестве X задано бинарное отношение σ, на множестве Y задано бинарное отношение τ. Отображение $\alpha : X \to Y$ называется *гомоморфизмом*, если оно сохраняет отношение, т. е. выполняется импликация $(x, y) \in \sigma \Rightarrow (x\alpha, y\alpha) \in \tau$. Гомоморфизм α называется *полустрогим*, если из $(x\alpha, y\alpha) \in \sigma$ следует, что существуют такие $t \in x\alpha\alpha^{-1}$, $u \in y\alpha\alpha^{-1}$, что $(t, u) \in \sigma$. Гомоморфизм α называется *локально строгим*, если из $(x\alpha, y\alpha) \in \sigma$ следует, что для каждого $t \in x\alpha\alpha^{-1}$ найдётся такое $u \in y\alpha\alpha^{-1}$, что $(t, u) \in \sigma$. Гомоморфизм α называется *квазистрогим*, если из $(x\alpha, y\alpha) \in \sigma$ следует, что существует такое $t \in x\alpha\alpha^{-1}$, что для каждого $u \in y\alpha\alpha^{-1}$ имеет место

соотношение $(t,u) \in \sigma$, и существует такое $u \in y\alpha\alpha^{-1}$, что для каждого $t \in x\alpha\alpha^{-1}$ имеет место соотношение $(t,u) \in \sigma$. Гомоморфизм α называется *строгим*, если из $(x\alpha, y\alpha) \in \sigma$ следует, что $(x,y) \in \sigma$.

Множество всех гомоморфизмов $\alpha : X \to Y$ обозначим $Hom(\sigma,\tau)$, всех полустрогих — $HHom(\sigma,\tau)$, всех локально строгих — $LHom(\sigma,\tau)$, всех квазистрогих — $QHom(\sigma,\tau)$, всех строгих обозначим $SHom(\sigma,\tau)$.

В работе [2] эти определения были переформулированы на языке булевых матриц. После исправления имеющихся в работе [2] недочётов формулировки выглядят следующим образом:

$$\alpha \in Hom(\sigma,\tau) \Leftrightarrow \sigma\alpha \subseteq \alpha\tau;$$

$$\alpha \in HHom(\sigma,\tau) \Leftrightarrow \sigma\alpha \subseteq \alpha\tau \wedge (\tau \cap im\alpha \times im\alpha) \subseteq \alpha^{-1}\sigma\alpha;$$

$$\alpha \in LHom(\sigma,\tau) \Leftrightarrow \sigma\alpha \subseteq \alpha\tau \wedge (\tau \cap im\alpha \times im\alpha)\,\alpha \subseteq \sigma\alpha;$$

$$\alpha \in SHom(\sigma,\tau) \Leftrightarrow \alpha\tau\alpha^{-1} = \sigma.$$

Обобщим определения на случай n-арных отношений. Множество X с заданным на нём n-арным отношением можно назвать ориентированным гиперграфом. Отличие от классического определения гиперграфа [3] в том, что в нашем случае ребро — это *упорядоченный* набор вершин.

Для любого множества A обозначим через Δ_A отношение равенства на A. Произвольное отношение $\alpha \subseteq X \times Y$ является *частичным* отображением $X \to Y$ тогда и только тогда, когда $\alpha^{-1}\alpha \subseteq \Delta_Y$. Отношение $\alpha \subseteq X \times Y$ является *многозначным полным* отображением $X \to Y$ тогда и только тогда, когда $\Delta_X \subseteq \alpha\alpha^{-1}$. Пусть на множестве X задано n-арное отношение σ, на множестве Y задано n-арное отношение τ. Частичное отображение $\alpha : X \to Y$ назовём *гомоморфизмом*, если выполняется импликация $(x_1,...,x_n) \in \sigma \cap (dom\alpha)^n \Rightarrow (x_1\alpha,...,x_n\alpha) \in \tau$. Многозначное полное отображение $\alpha : X \to Y$ назовём *гомоморфизмом*, если для любых $x_1,...,x_n \in X$ и $y_1,...,y_n \in Y$ выполняется импликация $(x_1,...,x_n) \in \sigma, y_1 = x_1\alpha,...,y_n = x_n\alpha \Rightarrow (y_1,...,y_n) \in \tau$. Гомоморфизм α назовём *строгим*, если из $(x_1\alpha,...,x_n\alpha) \in \tau$ следует, что $(x_1,...,x_2) \in \sigma$. Гомоморфизм α назовём *полустрогим*, если из $(x_1\alpha,...,x_n\alpha) \in \tau$ следует, что существуют такие $t_1 \in x_1\alpha\alpha^{-1}$, ..., $t_n \in x_n\alpha\alpha^{-1}$, что $(t_1,...,t_n) \in \sigma$. Запишем эти определения на языке матриц.

Теорема 1. *Частичное отображение $\alpha : X \to Y$ является гомоморфизмом тогда и только тогда, когда*

$$(\sigma \cap (dom\alpha)^n)_{i_1...i_n} \leq \vee_{j_1...j_n} \alpha_{i_1 j_1}...\alpha_{i_n j_n}\tau_{j_1...j_n}.$$

Теорема 2. *Многозначное полное отображение $\beta : X \to Y$ является гомоморфизмом тогда и только тогда, когда*

$$\vee_{i_1 \dots i_n} \beta_{i_1 j1} \cdots \beta_{i_n jn} \sigma_{i_1 \dots i_n} \leq \tau_{j_1 \dots j_n}.$$

Теорема 3. *Пусть $\gamma : X \to Y$ — гомоморфизм (частичный или многозначный полный). Тогда:*
1) *γ строгий в том и только в том случае, если*

$$(\sigma \cap (dom\alpha)^n)_{i_1 \dots i_n} \geq \vee_{j_1 \dots j_n} \gamma_{i_1 j1} \cdots \gamma_{i_n jn} \tau_{j_1 \dots j_n};$$

2) *γ полустрогий в том и только в том случае, если*

$$\vee_{i_1 \dots i_n} \gamma_{i_1 j1} \cdots \gamma_{i_n jn} \sigma_{i_1 \dots i_n} \geq (\tau \cap (im\gamma)^n)_{j_1 \dots j_n}.$$

Пусть $\sigma = \tau$. Тогда естественно рассмотреть следующие виды эндоморфизмов:

$$\alpha \in H'End(\sigma) \Leftrightarrow \tau = \alpha^{-1} \sigma \alpha;$$

$$\alpha \in L'End(\sigma) \Leftrightarrow \sigma\alpha = \alpha\tau.$$

Они образуют моноиды. В работе [1] было показано, что полустрогие, квазистрогие и локально строгие эндоморфизмы не образуют моноидов. Известно [1], что

$$SHom' \subseteq QHom \subseteq LHom \subseteq HHom \subseteq Hom.$$

Очевидно, что $L'End \subseteq LHom, H'End \subseteq HHom$. Оказывается, что в общем случае

$$L'End \cap (HHom \backslash LHom) = \emptyset;$$

$$(H'End \backslash HHom) \subseteq L'End.$$

Список литературы

1. Boettcher M., Knauer U. Endomorphism spectra of graphs // Discrete Mathematics. — 1992. — V. 109. — P. 45–57.
2. Ярошевич В. А. Отображения, согласующиеся с бинарными отношениями // Мат. вестник педвузов и ун-тов Волго-Вятского региона. — 2009. — Вып. 11. — С. 135–142.

3. Зыков А. А. Гиперграфы // Успехи мат. наук. — 1974. — Т. XXIX, вып. 6 (180). — С. 89–154.

О ЧИСЛЕ ЦИКЛОВ ДЛИНЫ m, $m \leq 6$, В РЕГУЛЯРНЫХ ТУРНИРАХ

С. В. Савченко (Черноголовка)

По определению, *турнир* является ориентацией полного графа. Пусть $c_m(T)$ — число циклов длины m (или, просто, m-циклов) в турнире T и $\beta_m(n)$ — максимальное число m-циклов в классе всех турниров порядка n. Точное значение величины $\beta_m(n)$ известно только для $m = 3$ и $m = 4$. В частности, используя чисто комбинаторные методы, М. Кендалл и Б. Бабингтон-Смит определили в [1] точное значение $\beta_3(n)$. Кроме того, было показано, что для нечетного n равенство $c_3(T) = \beta_3(n)$ имеет место только для *регулярного* турнира T порядка n, у которого, по определению, степень исхода каждой вершины совпадает с ее степенью захода и, следовательно, равна $\frac{n-1}{2}$. В свою очередь, при четном n максимум достигается на *почти регулярном* турнире, который, по определению, получается из некоторого регулярного турнира порядка $n + 1$ при помощи удаления одной из его вершин.

Случай $m = 4$ более сложен. Точное значение $\beta_4(n)$ первым нашел Ю. Коломбо. В соответствии с его статьей [2] максимальное число 4-циклов, возможное в турнире нечетного порядка n, достигается на единственном регулярном *локально транзитивном* турнире RLT_n порядка n. Пусть $N^+(v)$ — множество всех вершин в T, в которые идут дуги из вершины v, и $N^-(v)$ — множество всех вершин в T, из которых выходят дуги в вершину v. *Локальная транзитивность* означает, что для любой вершины v подмножества $N^+(v)$ и $N^-(v)$ индуцируют *транзитивные* турниры, которые, по определению, не содержат циклов. В свою очередь, можно показать (см. [3]), что минимум числа 4-циклов в классе всех регулярных турниров (нечетного) порядка n достигается тогда и только тогда, когда для любой вершины v в T подмножества $N^+(v)$ и $N^-(v)$ содержат максимальное число 3-циклов, т. е. индуцируют регулярный или почти регулярный турнир в соответствии с $n \equiv 3 \mod 4$ или $n \equiv 1 \mod 4$. По

определению, в первом случае T является *дважды регулярным* турниром DR_n, а во втором — *почти дважды регулярным* турниром NDR_n.

В нашем докладе на IX Международном семинаре "Дискретная математика и ее приложения" с помощью спектральных методов было показано, что

$$c_5(T) + 2c_4(T) = \frac{n(n-1)(n+1)(n-3)(n+3)}{160} \tag{1}$$

для любого регулярного турнира T порядка n. Вместе с упомянутыми выше результатами о числе 4-циклов эта формула позволяет получить следующую теорему о числе 5-циклов в T.

Теорема 1. *Пусть T — регулярный турнир порядка n. Тогда*

$$c_5(T) \le \begin{cases} \dfrac{n(n-1)(n+1)(n-2)(n-3)}{160}, & \text{если } n \equiv 3 \mod 4 \\ \dfrac{n(n-1)(n^3-4n^2+n-14)}{160}, & \text{если } n \equiv 1 \mod 4. \end{cases} \tag{2}$$

Эта оценка сверху достигается тогда и только тогда, когда турнир T является дважды регулярным (при $n \equiv 3 \mod 4$) или почти дважды регулярным (при $n \equiv 1 \mod 4$). Более того, также справедливо неравенство

$$\frac{n(n-1)(n+1)(n-3)(3n-11)}{480} \le c_5(T),$$

в котором равенство имеет место если и только если $T = RLT_n$.

Заметим, что для $m = 2, 3, 4, 5$ и произвольного турнира T величина $mc_m(T)$ совпадает со следом $tr_m(T)$ m-й степени матрицы смежности T. Однако, величина $6c_6(T)$ не равна $tr_6(T)$. Тем не менее, для регулярного турнира T порядка n соответствующая разность довольно просто выражается через n и $c_4(T)$.

Лемма 1. *Для регулярного турнира T порядка n справедливо равенство*

$$6c_6(T) = tr_6(T) - \frac{1}{64}n(n+1)(n-1)(3n^2-19) + 6c_4(T). \tag{3}$$

Так как $4c_4(T) = tr_4(T)$, формула (3) означает, что $c_6(T)$ является функцией спектра регулярного турнира T порядка n. Как известно (см. [4]), он состоит из перронова корня $\frac{n-1}{2}$ и собственных

значений вида $-\frac{1}{2}+i\rho_j$, где $j = 1, ..., n-1$. Это позволяет переписать формулу (3) следующим образом:

$$6c_6(T) = \frac{n(n-1)(n^4-8n^3+13n^2-9n-9)}{64} + \frac{21}{4}\sum_{j=1}^{n-1}\rho_j^4 - \sum_{j=1}^{n-1}\rho_j^6.$$

Равенство $tr_2(T) = 2c_2(T) = 0$ означает, что $\sum\limits_{j=1}^{n-1}\rho_j^2 = \frac{n(n-1)}{4}$. Таким образом, правило множителей Лагранжа позволяет получить следующую оценку сверху для $c_6(T)$.

Теорема 2. *Пусть T — регулярный турнир порядка $n \geq 7$. Тогда*

$$c_6(T) \leq \frac{n(n-1)(n+1)(n-3)(n^2-6n+3)}{384}.$$

При $n \geq 11$ эта оценка сверху достигается тогда и только тогда, когда турнир T является дважды регулярным.

Последнее предложение в утверждении теоремы 2 является следствием того факта, что для любого дважды регулярного турнира DR_n порядка $n \equiv 3 \mod 4$ справедливо равенство $\rho_j^2 = \frac{n}{4}$ при каждом $j = 1, ..., n-1$, и в силу [5] это спектральное свойство полностью характеризует дважды регулярный турнир в классе всех регулярных турниров порядка n.

Список литературы

1. Kendall M. G., Babington Smith B. On the method of paired comparisons // Biometrika. — 1940. — V. 33. — P. 239–251.

2. Colombo U. Sui circuiti nei grafi completi // Bollettino della Unione Matematica Italiana. — 1964. — V. 19. — P. 153–170.

3. Alspach B., Tabib C. A note on the number of 4-circuits in a tournament // Annals of Discrete Mathematics. — 1982. — V. 12. — P. 13–19.

4. Brauer A., Gentry I. C. On the characteristic roots of tournament matrices // Bulletin of the American Mathematical Society. — 1968. — V. 74. — P. 1133–1135.

5. Rowlison P. On 4-cycles and 5-cycles in regular tournaments // Bulletin of the London Mathematical Society. — 1986. — V. 18. — P. 135–139.

НОВЫЙ КЛАСС МЕТРИК ДЛЯ ВЕРШИН ГРАФА

П. Ю. Чеботарев (Москва)

Стандартное расстояние в графе — длина кратчайшего пути [1]. Используют также резисторное расстояние [2], равное коммутационному расстоянию (commute-time distance) для цепи Маркова [3].

В [4] построено семейство мер удаленности вершин графа, предельными элементами которого являются расстояние кратчайшего пути и резисторное расстояние. В реализованных авторами [4] алгоритмах кластерного анализа наилучшие результаты достигаются при использовании не крайних, а промежуточных элементов семейства, но ценность подхода снижается тем, что эти элементы не являются метриками: они нарушают неравенство треугольника.

В настоящей работе строится класс *логарифмических лесных метрик*, обладающий теми же предельными свойствами. Конструкция класса основана на матричной теореме о лесах [5] и неравенстве перемычки [6]. Полученные метрики удовлетворяют *геодезическому условию*: $d(i,j) + d(j,k) = d(i,k)$ тогда и только тогда, когда каждый путь из i в k проходит через j.

Пусть G — взвешенный мультиграф без петель с множествами вершин $V(G) = \{1,\dots,n\}$ $(n > 1)$ и ребер $E(G)$. Для $i,j \in V(G)$ пусть $n_{ij} \in \{0,1,\dots\}$ — число ребер в G, инцидентных i и j; для каждого $p \in \{1,\dots,n_{ij}\}$ $w_{ij}^p > 0$ — вес p-го ребра этого типа. Пусть $w_{ij} = \sum_{p=1}^{n_{ij}} w_{ij}^p$ (если $n_{ij} = 0$, то по определению $w_{ij} = 0$).

Корневое дерево — связный ациклический взвешенный граф с одной отмеченной вершиной, называемой *корнем*. *Корневой лес* — граф, все компоненты которого — корневые деревья. Корни этих деревьев называются корнями корневого леса. Под весом взвешенного графа H, $w(H)$, понимаем произведение весов его ребер. Если в H нет ребер, то $w(H) = 1$. Вес множества S графов, $w(S)$, есть сумма весов графов, принадлежащих S; вес пустого множества равен нулю.

Для данного взвешенного мультиграфа G через $\mathcal{F} = \mathcal{F}(G)$ и $\mathcal{F}_{ij} = \mathcal{F}_{ij}(G)$ обозначим соответственно множество всех остовных корневых лесов G и множество всех остовных корневых лесов G, в которых вершина i принадлежит дереву с корнем j. Пусть

$$f = w(\mathcal{F}),\ \ f_{ij} = w(\mathcal{F}_{ij}),\ \ i,j \in V(G).$$

$F = (f_{ij})_{n\times n}$ называют *матрицей лесов* мультиграфа G.

Пусть $L = (\ell_{ij})$ — лапласовская матрица G, т. е. $\ell_{ij} = -w_{ij}$ при $j \neq i$ и $\ell_{ij} = \sum_{k\neq i} w_{ik}$ при $j = i$. Рассмотрим матрицу $Q = (q_{ij}) =$

$(I+L)^{-1}$. В силу матричной теоремы о лесах (см., например, [5])

$$q_{ij} = f_{ij}/f, \quad i,j = 1,\dots,n.$$

Матрица Q может рассматриваться как *матрица близости* для вершин G [7].

Через $d^s(i,j)$ обозначим *расстояние кратчайшего пути*, т. е. число ребер в кратчайшем пути между i и j в G; $d^r(i,j)$ — *резисторное расстояние* между i и j, определяемое следующим образом:

$$d^r(i,j) = \ell^+_{ii} + \ell^+_{jj} - 2\ell^+_{ij},$$

где $(\ell^+_{ij})_{n\times n} = L^+$ — матрица, обобщенно обратная по Муру—Пенроузу к лапласовской матрице L мультиграфа G.

Введем новый класс метрик на множестве вершин графа. Пусть

$$Q_\alpha = (I+\alpha L)^{-1}, \tag{1}$$

где I — единичная матрица, $\alpha \in \mathbb{R}_+$ — параметр. Пусть

$$H_\alpha = \gamma\,(\alpha-1)\,\overrightarrow{\log_\alpha Q_\alpha}, \tag{2}$$

где $\alpha \neq 1$, $\gamma \in \mathbb{R}_+$, $\overrightarrow{\log_\alpha Q_\alpha}$ — покомпонентная операция. Рассмотрим

$$D_\alpha = \tfrac{1}{2}(h_\alpha \mathbf{1}^{\mathrm{T}} + \mathbf{1}h_\alpha^{\mathrm{T}}) - H_\alpha, \tag{3}$$

где h_α — столбец диагональных элементов H_α, $\mathbf{1} = (1,\dots,1)^{\mathrm{T}}$.

Определение (2) переносится на случай $\alpha = 1$ по непрерывности:

$$H_1 = \gamma\overrightarrow{\ln Q}, \tag{4}$$

Теорема 1. *Если G связен и $\alpha,\gamma > 0$, то матрица $D_\alpha = (d_{ij}(\alpha))$, определяемая (1)–(4), существует и задает метрику на $V(G)$.*

В силу теоремы 1 корректно следующее определение. Пусть G — связный мультиграф и $\alpha > 0$. *Логарифмической лесной метрикой с параметром α на G* назовем функцию d_α: $V(G)\times V(G) \to \mathbb{R}$ такую, что $d_\alpha(i,j) = d_{ij}(\alpha)$, где $(d_{ij}(\alpha)) = D_\alpha$ — матрица, определяемая (1)–(4).

Элементы матрицы расстояний D_α могут быть выражены через веса остовных лесов в G. Через G_α обозначим взвешенный мультиграф, получающийся из G умножением весов его ребер на α. Пусть

$$f_{ij}(\alpha) = w(\mathcal{F}_{ij}(G_\alpha)), \quad i,j = 1,\dots,n.$$

Предложение 1. *Если G связен и $\alpha,\gamma > 0$, то элементы матрицы $D_\alpha = (d_{ij}(\alpha))$, определяемой (1)–(4), имеют представление*

$$d_{ij}(\alpha) = \begin{cases} \gamma\,(\alpha-1)\log_\alpha \frac{\sqrt{f_{ii}(\alpha)\,f_{jj}(\alpha)}}{f_{ij}(\alpha)}, & \alpha \neq 1 \\ \gamma \ln \frac{\sqrt{f_{ii}\,f_{jj}}}{f_{ij}}, & \alpha = 1 \end{cases}, \quad i,j = 1,\ldots,n.$$

Для мультиграфа G функция $d : V(G) \times V(G) \to \mathbb{R}$ *геодезична*, если для всех $i,j,k \in V(G)$ $d(i,j)+d(j,k)=d(i,k)$ выполняется тогда и только тогда, когда каждый путь из i в k содержит j.

Теорема 2. *Если G связен и $\alpha > 0$, то метрика $d_\alpha(i,j)$ геодезична.*

Рассмотрим введенные метрики со шкалирующим множителем

$$\gamma = \ln(e + \alpha^{\frac{2}{n}}). \tag{5}$$

Теорема 3. *Если G связен, то метрика $d_\alpha(i,j)$ со шкалирующим множителем* (5) *сходится к метрике кратчайшего пути $d^s(i,j)$ при $\alpha \to 0^+$ и к резисторной метрике $d^r(i,j)$ при $\alpha \to \infty$.*

Для метрик с произвольным положительным γ "сходится к" в теореме 3 нужно заменить на "в пределе пропорциональна".

Работа выполнена при поддержке РФФИ (проект 09-07-00371-а) и Программы Президиума РАН "Математическая теория управления".

Список литературы

1. Buckley F., Harary F. Distance in Graphs. — Redwood City: Addison-Wesley, 1990.

2. Klein D. J., Randić M. Resistance distance // Journal of Mathematical Chemistry. — 1993. — V. 12. — P. 81–95.

3. Tetali P. Random walks and the effective resistance of networks // Journal of Theoretical Probability. — 1991.— V. 4. — С. 101–109.

4. Yen L., Saerens M., Mantrach A., Shimbo M. A family of dissimilarity measures between nodes generalizing both the shortest-path and the commute-time distances // 14th ACM SIGKDD International Conference on Knowledge Discovery & Data Mining, 2008. — P. 785–793.

5. Chebotarev P., Agaev R., Forest matrices around the Laplacian matrix // Linear Algebra and its Applications. — 2002. — V. 356. — P. 253–274.

6. Chebotarev P. A graph bottleneck inequality / arXiv preprint math.CO/0810.2732, 2008. — http://arxiv.org/abs/0810.2732.

7. Chebotarev P. Spanning forests and the golden ratio // Discrete Applied Mathematics. — 2008. — V. 156. — P. 813–821.

ОБ АСИМПТОТИЧЕСКОМ ПОВЕДЕНИИ ПРЕДПИСАННОГО ХРОМАТИЧЕСКОГО ЧИСЛА ПОЛНЫХ МНОГОДОЛЬНЫХ ГРАФОВ

Д. А. Шабанов (Москва)

В докладе рассматривается асимптотическое поведение предписанного хроматического числа полных многодольных графов с одинаковым размером долей. Сначала напомним основные определения.

Пусть $G = (V, E)$ — некоторый граф и задано конечное множество C, называемое множеством *цветов*. *Вершинным предписанием* A называется любое отображение, которое каждой вершине $v \in V$ ставит в соответствие некоторое (непустое) подмножество $A(v) \subseteq C$. Если $|A(v)| = r$ для любой вершины $v \in V$, то говорят, что *мощность* предписания равна r.

Раскраской f вершин графа G, соответствующей предписанию A, называется такое однозначное отображение $f : V \to C$, что $f(v) \in A(v)$ для любого $v \in V$. Раскраска называется *правильной* для графа G, если в этой раскраске все ребра графа неодноцветны. Граф называется *предписанно r-раскрашиваемым*, если для любого множества цветов C и любого вершинного предписания A мощности r найдется правильная раскраска, соответствующая данному предписанию. *Предписанным хроматическим числом* графа G называется такое минимальное натуральное число r, что G является предписанно r-раскрашиваемым.

Изучение предписанного хроматического числа было инициировано работами В. Г. Визинга [1], а также П. Эрдеша, А. Л. Рубина и Х. Тейлора [2]. Для предписанного хроматического числа графа G будем использовать обозначение $ch(G)$.

Обозначим через $K_{m*r} = K_{m,\dots,m}$ полный r-дольный граф с одинаковым размером долей m. Эрдеш, Рубин и Тейлор поставили задачу о нахождении предписанного хроматического числа этого графа. Легко проверить, что $ch(K_{1*r}) = r$ и $ch(K_{m*1}) = 1$. Эрдеш, Рубин и Тейлор доказали [2], что $ch(K_{2*r}) = r$. Х. Киерстед показал [3], что $ch(K_{3*r}) = \lceil (4r-1)/3 \rceil$.

Для больших значений параметра m точное значение $ch(K_{m*r})$ неизвестно, но были получены достаточно хорошие оценки. Н. Алон [4] доказал, что $ch(K_{m*r}) = \Theta(r \ln m)$, т. е. существуют такие положительные константы c_1 и c_2, что для всех $m \geq 2$, $r \geq 2$ выполняются неравенства

$$c_1\, r \ln m \leq ch(K_{m*r}) \leq c_2\, r \ln m.$$

А. Рубин [2] нашел асимптотику $ch(K_{m*2})$ при $m \to \infty$:

$$ch(K_{m*2}) = (1 + o(1)) \log_2 m.$$

Наконец, М. Кривелевич и Н. Газит [5] показали, что при фиксированном r и $m \to \infty$ выполнено

$$ch(K_{m*r}) = (1 + o(1)) \frac{\ln m}{\ln (r/(r-1))}. \qquad (1)$$

Основным результатом работы является нахождение асимптотического поведения величины $ch(K_{m*r})$ при $m, r \to \infty$. Справедлива следующая теорема.

Теорема 1. *Пусть $r = r(m)$ — функция, удовлетворяющая условию $\ln r = o(\ln m)$ при $m \to \infty$. Тогда*

$$ch(K_{m*r}) = (1 + o(1)) \frac{\ln m}{\ln (r/(r-1))}.$$

Полученный в теореме 1 результат расширяет асимптотику (1), полученную Кривелевичем и Газитом, на случай растущих функций $r = r(m)$.

Доказательство теоремы 1 опирается на тесную связь между предписанными раскрасками полных r-дольных графов и полноцветными r-раскрасками гиперграфов. Напомним, что гиперграф называется *n-равномерным*, если каждое его ребро содержит ровно n вершин. Раскраска множества вершин гиперграфа $H = (V, E)$ в r цветов (r-раскраска) называется *полноцветной*, если в ней каждое ребро из E содержит вершины всех цветов. В работе А. В. Косточки [6] была поставлена задача об отыскании величины $p(n, r)$, равной минимальному числу ребер гиперграфа в классе n-равномерных гиперграфов, не допускающих полноцветных r-раскрасок. А. В. Косточка показал [6], что

$$p(n, r) \le N(r, n) \le r\, p(n, r), \qquad (2)$$

где через $N(r, n)$ обозначено минимальное число вершин графа в классе полных r-дольных графов, предписанное хроматическое число которых превышает n. Неравенства (2) в частном случае $r = 2$ были получены еще Эрдешем, Рубином и Тейлором в [2]. С помощью этих соотношений можно доказать следующую лемму, проясняющую связь величин $ch(K_{m*r})$ и $p(n, r)$.

Лемма 1. *Для любых r и m выполняются неравенства*

$$p\left(ch(K_{m*r})-1,r\right)\leq rm<r\,p\left(ch(K_{m*r}),r\right).$$

Чтобы вывести теорему 1 из леммы 1, необходимо оценить величину $p(n,r)$. Оценки $p(n,r)$ при произвольных значениях n и r получены в теореме 2.

Теорема 2. *Существует такая положительная константа C, что для любых $r\leq n$ выполнены неравенства*

$$\frac{1}{r}\left(\frac{r}{r-1}\right)^n\leq p(n,r)\leq Cn^2\left(\frac{r}{r-1}\right)^n.$$

Работа выполнена при финансовой поддержке РФФИ (грант 09-01-00294), программы "Ведущие научные школы" (код проекта НШ–8784.2010.1), гранта Президента РФ (МК – 3429.2010.01).

Список литературы

1. Визинг В. Г. Раскраска вершин графа в предписанные цвета // Методы дискретного анализа в теории кодов и схем: сборник научных трудов. Т. 29. — Новосибирск: Изд-во Института математики СО АН СССР, 1976. — С. 3–10.

2. Erdős P., Rubin A. L., Taylor H. Choosability in graphs // Proc. West Coast Conference on Combinatorics, Graph Theory and Computing. — 1979. — 26. — P. 125–157.

3. Kierstead H. On the choosability of complete multipartite graphs with size part 3 // Discrete Mathematics. — 2000. — V. 211. — P. 255–259.

4. Alon N. Choice number of graphs: a probabilistic approach // Combinatorics, Probability and Computing. — 1992. — V. 1. — P. 107–114.

5. Gazit N., Krivelevich M. On the asymptotic value of the choice number of complete multi-partite graphs // Journal of Graph Theory. — 2006. — V. 52. — P. 123–134.

6. Kostochka A. V. On a theorem by Erdős, Rubin and Taylor on choosability of complete bipartite graphs // Electronic Journal of Combinatorics. — 2002. — V. 9.

О СВЯЗНОСТИ СЛУЧАЙНЫХ ДИСТАНЦИОННЫХ ГРАФОВ СПЕЦИАЛЬНОГО ВИДА

А. Р. Ярмухаметов (Москва)

В 1959 году П. Эрдеш и А. Реньи предложили следующую модель случайного графа [1, 2]: рассматривается вероятностное пространство

$$G(N,p) = (\Omega_N, \mathcal{F}_N, \mathcal{P}_{N,p}),$$

где Ω_N — множество всех графов $G = (V,E)$ на N вершинах без петель, кратных ребер и ориентации (т. е. $|\Omega_N| = 2^{C_N^2}$), $\mathcal{F}_N = 2^{\Omega_N}$,

$$\mathcal{P}_{N,p}(G) = p^{|E|}(1-p)^{C_N^2 - |E|},\ p \in (0,1).$$

Иными словами, мы проводим то или иное ребро между вершинами случайного графа с вероятностью p независимо от остальных ребер.

Определение. Будем говорить, что случайный граф обладает некоторым свойством *асимптотически почти наверное* (кратко *а.п.н.*), если вероятностная мера множества графов, обладающих этим свойством, стремится к 1 при $N \to \infty$. Отметим, что вероятность ребра p есть, вообще говоря, функция от N.

В работах Эрдеша и Реньи были получены следующие результаты:

1. Величина $p^* = \frac{\ln N}{N}$ является "пороговой вероятностью" для свойства связности случайного графа, т. е. при $p \geq cp^*$ (где $c > 1$) случайный граф в пространстве $G(N,p)$ а.п.н. связен, а при $p \leq cp^*$ (где $c < 1$) случайный граф а.п.н. не связен;

2. Величина $p_1^* = \frac{1}{N}$ является "пороговой вероятностью" для существования "гигантской компоненты" в случайном графе, а именно: если $p \leq \frac{c}{N}$ (где $c < 1$), то а.п.н. случайный граф в пространстве $G(N,p)$ будет состоять из компонент, количество вершин в каждой из которых равно $O(\ln N)$; если же $p \geq \frac{c}{N}$ (где $c > 1$), то случайный граф а.п.н. будет содержать "гигантскую компоненту" размера $\Omega(N)$ (при этом все остальные вершины будут содержаться в компонентах размера $O(\ln N)$).

Введем новое пространство случайных графов, которое будем называть *пространством случайных дистанционных графов*. Для этого положим $n = 4k$, $k \in \mathbb{N}$, $N = C_n^{n/2}$ и рассмотрим *полный дистанционный граф* $\mathcal{G}_N = (\mathcal{V}_N, \mathcal{E}_N)$, у которого

$$\mathcal{V}_N = \left\{ \mathbf{x} = (x_1, \ldots, x_n) : x_i \in \{0,1\}, x_1 + \ldots + x_n = 2k = \frac{n}{2} \right\},$$

$$\mathcal{E}_N = \left\{ \{\mathbf{x}, \mathbf{y}\} \in \mathcal{V}_N \times \mathcal{V}_N : (\mathbf{x}, \mathbf{y}) = k = \frac{n}{4} \right\}.$$

Таким образом, вершины полного дистанционного графа являются точками из $\{0,1\}^n$ и этих вершин ровно N. При этом ребра графа $\mathcal{G}_N$ суть пары его вершин, удаленные друг от друга на расстояние $\sqrt{\frac{n}{2}}$. Именно этим и обусловлено название графа. Рассмотрение подобных графов глубоко мотивировано задачами комбинаторной геометрии [3, 4].

Определим новое вероятностное пространство

$$\mathcal{G}^{dist}(N,p) = (\Omega_N^{dist}, \mathcal{F}_N^{dist}, \mathcal{P}_{N,p}^{dist}),$$

где Ω_N^{dist} — множество всех остовных подграфов $G = (\mathcal{V}_N; E)$ полного дистанционного графа $\mathcal{G}_N$, $\mathcal{F}_N^{dist} = 2^{\Omega_N^{dist}}$,

$$\mathcal{P}_{N,p}^{dist}(G) = p^{|E|}(1-p)^{|\mathcal{E}_N|-|E|},\ p \in (0,1).$$

Несмотря на близость модели, рассматриваемой в данной работе, и классической модели Эрдеша—Реньи случайных графов, между ними имеются существенные различия.

Сформулируем результаты для графа $\mathcal{G}^{dist}(N,p)$ о "пороговой вероятности связности" и о нижней границе "наличия гигантской компоненты".

Теорема 1. *Пусть* $p_* = \frac{\sqrt{\pi}}{2\sqrt{2\ln 2}} \frac{(\ln N)^{3/2}}{N}$. *Тогда:*

а) при $p \geq cp_*$, *где* $c > 1$, *случайный граф в пространстве* $\mathcal{G}^{dist}(N,p)$ *а.п.н. связен;*

б) при $p \leq cp_*$, *где* $c < 1$, *случайный граф в пространстве* $\mathcal{G}^{dist}(N,p)$ *а.п.н. не связен.*

Теорема 2. *Пусть* $p_{**} = \frac{\sqrt{\pi}}{2\sqrt{2\ln 2}} \frac{(\ln N)^{1/2}}{N}$. *Тогда при* $p \leq cp_{**}$, *где* $c < 1$, *случайный граф в пространстве* $\mathcal{G}^{dist}(N,p)$ *а.п.н. будет состоять из компонент, количество вершин в каждой из которых не превышает* $O(\ln N)$.

Список литературы

1. Алон Н., Спенсер Дж. Вероятностный метод. — М.: Бином, 2007.

2. Erdős P., Rényi A. On the evolution of random graphs // Magyar Tud. Akad. Mat. Kutató Int. Közl. — 1960. — 5. — С. 17–61.

3. Райгородский А. М. Линейно-алгебраический метод в комбинаторике. — М.: МЦНМО, 2007.

4. Райгородский А. М. Проблема Борсука и хроматические числа некоторых метрических пространств // УМН, 56. — 2001. — 1 (337). — С. 107–146.

5. Bollobas B. Random Graphs. — New York: Academic Press, 1985.

6. Колчин В. Ф. Случайные графы. — М.: Физматлит, 2004.

7. Karp R. The transitive closure of a random digraph // Random structures and Algorithms. — 1990. — 1. — С. 73–94.

Секция «Математическая теория интеллектуальных систем»

О КОДИРОВАНИИ ИЗОБРАЖЕНИЙ, ИНВАРИАНТНОМ ОТНОСИТЕЛЬНО ПРОЕКТИВНЫХ ПРЕОБРАЗОВАНИЙ

Д. В. Алексеев (Москва)

Кодирование геометрических образов используется в геометрической теории распознавания образов. Результаты, относящиеся к кодированию, инвариантному относительно движений, преобразований подобия и аффинных преобразований были получены ранее В. Н. Козловым [1, 2].

Определение. Ориентированным углом $\angle AOB$ будем называть величину α, если поворот на угол $0 \leq \alpha \leq \pi$ в положительном направлении (т.е. против часовой стрелки) относительно точки O переводит луч OA в луч OB и $\angle AOB = -\alpha$ если поворот на угол α в отрицательном направлении (т.е. по часовой стрелке) переводит луч OA в луч OB.

Определение. Двойным отношением лучей OA, OB, OC и OD называют величину $[A, B, C, D]_O = \frac{\sin \angle AOC}{\sin \angle BOC} : \frac{\sin \angle AOD}{\sin \angle BOD}$, где все углы рассматриваются как ориентированные. Если же какой либо из знаменателей обращается в ноль будем обозначать это (формально) $[A, B, C, D]_O = \infty$.

Определение. *Проективной плоскостью* $\overline{\Pi}$ будем называть множество $\mathbf{R}^3 \setminus \{(0, 0, 0)\}$, причем наборы (x, y, z) и (kx, ky, kz), $(k \neq 0)$ соответствуют одной и той же точке проективной плоскости. Геометрически проективная плоскость представляет собой объединение плоскости и множества бесконечно удаленных точек, образующих бесконечно удаленную прямую.

Определение. *Проективным* будем называть преобразование которое переводит $(x, y, z) \mapsto (x, y, z)A$, $(\det A \neq 0)$.

Замечание 1. Корректность определения очевидна: $(kx, ky, kz) \mapsto (x, y, z)A \cdot k$.

Замечание 2. Геометрический смысл проективных преобразований подробно излагается в [4–6].

Определение. Пусть A — конечное множество точек проективной плоскости. Пусть задана биекция $M : A \leftrightarrow \{1, 2, \ldots, n\}$ — нумерация точек и кодирующая функция $T : \overline{\Pi}^n \mapsto \mathbf{R}^{n \cdot C_{n-1}^4}$, ставящая множеству A в соответствие множество

$$\rho_{s;\, i,j,k,l} = [M^{-1}(i), M^{-1}(j), M^{-1}(k), M^{-1}(l)]_{M^{-1}(s)}$$

— двойные отношения четверок прямых, для тех пятерок, для которых указанные величины определены. *Кодом* изображения A будем называть пару $< M, T(A, M) >$.

Определение. Изображения A и B будем называть *эквивалентными* относительно кодирующей функции T, если существуют нумерации M_1 и M_2, такие, что $T(A, M_1) = T(B, M_2)$.

Определение. Изображения A и B будем называть *проективно эквивалентными* (π-*эквивалентными*), если существует проективное преобразование $\mathcal{P} : A \mapsto B$.

Определение. Изображение A будем называть *плоским проективным изображением*, если не существует трех прямых l_1, l_2 и l_3 таких, что $A \subset l_1 \cup l_2 \cup l_3$.

Теорема. *Плоские проективные изображения эквивалентны тогда и только тогда, когда они π–эквивалентны.*

Лемма 1 [3]. *Пусть $\mathcal{P}$ — проективное преобразование, и точки O, A, B, C, D таковы, что никакие две прямые из OA, OB, OC и OD не совпадают. Тогда $[A, B, C, D]_O = [\mathcal{P}(A), \mathcal{P}(B), \mathcal{P}(C), \mathcal{P}(D)]_{\mathcal{P}(O)}$. Другими словами, двойное отношение инвариантно относительно проективных преобразований.*

Лемма 2 [4]. *Пусть заданы две четверки точек $A_1, A_2, A_3, A_4 \in \overline{\Pi}$ и $B_1, B_2, B_3, B_4 \in \overline{\Pi}$ так, что никакие три не лежат на одной прямой. Тогда существует единственное проективное преобразование $\mathcal{P}$, такое, что $\mathcal{P}(A_i) = B_i$, $i = 1, 2, 3, 4$.*

Лемма 3. *Пусть заданы точки O, A, B, C, так, что никакие три не лежат на одной прямой и число $\kappa \in \mathbf{R}$. Тогда геометрическим местом точек X таких, что $[A, B, C, X]_O = \kappa$ является $l \setminus \{O\}$, где l — некоторая прямая, проходящая через точку O.*

Лемма 4. 1) Если $[A, B, C, D]_O = 1$, то точки A, O, B, или C, O, D лежат на одной прямой. 2) Если $[A, B, C, D]_O = 0$, то точки A, O, C или B, O, D лежат на одной прямой. 3) Если $[A, B, C, D]_O$ не определено, то точки B, O, C или A, O, D лежат на одной прямой.

Лемма 5. *Пусть известен код плоского проективного изображения A. Тогда существует алгоритм, позволяющий для любой тройки точек определить, лежат ли они на одной прямой или нет.*

Доказательство (теоремы). Из леммы 1 сразу же вытекает, что если A и B проективно эквивалентны, то они эквивалентны и относительно кодирующей функции T.

Докажем в обратную сторону. Рассмотрим точки A_i, $i = 1, 2, 3, 4$ никакие три из которых не лежат на одной прямой. Такая четверка всегда существует, т.к. A — плоское проективное изображение. Пусть им соответствуют точки B_i i=1,2,3,4. По лемме 2 найдется проективное преобразование $\mathcal{P}$, переводящее A_i в B_i, i=1,2,3,4. Рассмотрим произвольную точку $A' \in A$. Рассмотрим следующие случаи: A' не лежит на прямых A_1A_2, A_1A_3 и A_1A_4. Тогда двойное отношение $\kappa = [A'A_2A_3A_4]_{A_1}$ определено и не равно 0. По лемме 1 таким же будет и $[\tilde{B}B_2B_3B_4]_{B_1} = \kappa$, где $\tilde{B}$ — образ A' при проективном преобразовании $\mathcal{P}$. Но по лемме 3 из этого следует, что точка $\tilde{B}$ должна лежать на прямой $l' = B_1B'$, где $B' \in B$ — точка, соответствующая A'. Если точка $\tilde{B}$ лежит на какой–либо прямой $\tilde{l}$, соединяющих данные точки, но не проходящей, через A_1, то точка B' тоже должна лежать на этой прямой $\tilde{l}$. Таким образом $\tilde{B} = B' = l' \cap \tilde{l}$, что и требовалось доказать.

Автор выражает свою признательность В. Б. Кудрявцеву и В. Н. Козлову за постановку задачи и внимание к работе.

Список литературы

1. Козлов В. Н. Элементы математической теории зрительного восприятия. — М.: Изд. ЦПИ при мех.-мат. ф-те МГУ, 2001.

2. Козлов В. Н. О кодировании дискретных фигур // Дискретная математика. — 1996. — Т. 8, вып. 4. — С. 57–61.

3. Клейн Ф. Элементарная математика с точки зрения высшей. Том 2. Геометрия. — М: Наука, Главн. ред. физ.-мат. лит., 1987.

4. Юнг Дж. В. Проективная геометрия. — М.: ИЛ, 1949.

5. Ефимов Н. В. Высшая геометрия. — М.: Физматлит, 2003.

6. Кокстер Х. С. М. Действительная проективная плоскость. — М: Гос. изд-во физ.-мат. лит., 1959.

АВТОМАТЫ В p-АДИЧЕСКОМ РАКУРСЕ

В. С. Анашин (Москва)

Под автоматом мы везде далее понимаем инициальный автомат Мили (не обязательно с конечным числом состояний), входной и выходной алфавиты которого совпадают и состоят из p символов

(чисел) $0, 1, \ldots, p-1$, где p — простое число. Каждый автомат естественным образом задает отображение множества $\mathbb{Z}_p$ всех (односторонне) бесконечных последовательностей в $\mathbb{Z}_p$. Как известно, такие отображения называются *детерминированными функциями*, причем детерминированная функция называется *ограниченно детерминированной*, если она может быть задана автоматом с конечным числом состояний. Множество $\mathbb{Z}_p$ естественным образом наделяется структурой кольца целых p-адических чисел, т. е. превращается в метрическое пространство заданием метрики $|a-b|_p$, $a, b \in \mathbb{Z}_p$, где $|\ |_p$ — p-адическая (т. е., неархимедова) норма, и, кроме того, становится измеримым пространством с естественной вероятностной мерой, в качестве которой выступает мера Хаара μ, нормированная так, чтобы $\mu(\mathbb{Z}_p) = 1$. Напомним, что любое целое p-адическое число $a \in \mathbb{Z}_p$ единственным образом может быть представлено в канонической форме $a = \sum_{i=0}^{\infty} \alpha_i \cdot p^i$, $\alpha_i \in \{0, 1, \ldots, p-1\}$, а тогда $|a|_p = p^{-\min\{i:\, a_i \neq 0\}}$, и $|a|_p = 0$, если все $\alpha_i = 0$ (т.е. если $a = 0$). Можно показать (см., например, [1]), что *все детерминированные функции* $f\colon \mathbb{Z}_p \to \mathbb{Z}_p$, *и только они, удовлетворяют* p*-адическому условию Липшица с константой* 1, т.е. $|f(a) - f(b)|_p \leqslant |a-b|_p$ для любых $a, b \in \mathbb{Z}_p$. В частности, все детерминированные функции непрерывны относительно p-адической метрики. Например, детерминированными являются все функции, задаваемые полиномами с целыми p-адическими (в частности, рациональными целыми) коэффициентами. Отметим, что в случае $p = 2$ стандартные команды процессора, такие как OR, поразрядное логическое "или", XOR, поразрядное логическое "исключительное или" (т. е. поразрядное сложение по модулю 2), AND, поразрядное логическое "и" (т. е. поразрядное умножение по модулю 2), и т. п. естественным образом продолжаются до функций из $\mathbb{Z}_2 \times \mathbb{Z}_2$ в $\mathbb{Z}_2$ (т.е. до функций двух целых 2-адических аргументов), которые удовлетворяют (2-мерному) условию Липшица с константой 1. Отсюда, в частности, следует, что все функции, полученные с помощью композиций стандартных арифметических и поразрядных логических команд процессора могут рассматриваться как 2-адические детерминированные функции. Например, функция $f(x) = x + (x^2 \,\mathsf{OR}\, c)$ при любом $c \in \mathbb{Z}_2$ удовлетворяет условию Липшица с константой 1. Заметим, что если c является отрицательным рациональным целым числом (т.е. в канонической 2-адической форме представления c содержится не более конечного числа нулевых слагаемых), то функция f является ограниченно-детерминированной.

В свете сказанного, p-адический анализ может оказаться весь-

ма эффективным "аналитическим" инструментом изучения свойств детерминированных функций и поведения автоматов, что и было продемонстрировано в [1]. Например, *автомат обратим* (т.е. индуцирует перестановку каждого множества $\mathbb{Z}/p^n\mathbb{Z}_p = \{0, 1, \ldots, p^n - 1\}$ всех слов длины n в алфавите $\mathbb{Z}/p\mathbb{Z} = \{0, 1, \ldots, p-1\}$ для всех $n = 1, 2, 3, \ldots$) *тогда и только тогда, когда задаваемая им детерминированная функция сохраняет меру* μ. Это общее утверждение дает возможность доказывать обратимость конкретных автоматов. Например, автомат, задающий функцию, которая является полиномом над $\mathbb{Z}_p$ (в частности, над кольцом $\mathbb{Z}$ рациональных целых чисел), обратим тогда и только тогда, когда он индуцирует перестановку на множестве $\mathbb{Z}/p^2\mathbb{Z}$ всех слов длины 2. Это же верно, например, и для автомата, задающего функцию $f(x) = x + (x^2 \,\mathsf{OR}\, c)$.

Напомним, что множество $\mathcal{F}$ преобразований (непустого) множества M наз. *транзитивным*, если для любых $a, b \in M$ найдется $f \in \mathcal{F}$ такое, что $f(a) = b$. Преобразование f множества M наз. транзитивным, если транзитивно множество $\{e = f^0, f = f^1, f^2, \ldots\}$, где $f^i(x) = \underbrace{f(f(\ldots(f}_{i \text{ раз}}(x)\ldots)$, e — тождественное преобразование. Взаимно-однозначное преобразование f наз. транзитивным, если транзитивно множество $\{e, f^{\pm 1}, f^{\pm 2}, \ldots\}$, где f^{-1} — преобразование, обратное к f. В свете сказанного, обратимый автомат естественно назвать транзитивным, если он задает транзитивное преобразование каждого множества $\mathbb{Z}/p^n\mathbb{Z}$ всех слов длины n, $n = 1, 2, 3 \ldots$ В [1] показано, что *автомат транзитивен тогда и только тогда, когда задаваемая им детерминированная функция* $f\colon \mathbb{Z}_p \to \mathbb{Z}_p$ *эргодична относительно меры* μ. С помощью этого общего критерия можно доказать, например, что автомат, задающий полином над $\mathbb{Z}_p$, транзитивен тогда и только тогда, когда он задает транзитивное преобразование множества всех слов длины 3; это же верно и для автомата, задающего функцию $x + (x^2 \,\mathsf{OR}\, c)$, где $c \in \mathbb{Z}_p$.

Возможен, однако, и другой подход к определению понятия "транзитивный автомат". Будем рассматривать только те автоматы, каждое состояние s из множества S всех внутренних состояний автомата достижимо из начального состояния s_0, т. е. автомат перейдет из s_0 в s при подаче на вход некоторого конечного входного слова. Каждый автомат $\mathfrak{A}$ задает семейство автоматов $\mathfrak{A}_s$, $s \in S$, где $\mathfrak{A}_s$ отличается от $\mathfrak{A}$ только тем, что у него другое начальное состояние, s вместо s_0. Автомат $\mathfrak{A}$ наз. *вполне транзитивным*, если семейство детерминированных функций, задаваемых семейством автоматов $\mathfrak{A}_s$, $s \in S$, является транзитивным на каждом множе-

стве $\mathbb{Z}/p^n\mathbb{Z}$ для всех $n = 1, 2, 3, \ldots$ (т.е. для любых двух конечных слов v и w одинаковой длины найдется автомат $\mathfrak{A}_s$, преобразующий v в w). Автомат $\mathfrak{A}$ наз. *абсолютно транзитивным*, если каждый автомат $\mathfrak{A}_s$, $s \in S$, вполне транзитивен. Автомату $\mathfrak{A}$ сопоставим замыкание (в топологии евклидовой плоскости) $\mathcal{A}_{2\mathfrak{l}}$ всех точек вида $(\frac{v}{p^n}, \frac{w}{p^n})$ единичного квадрата $[0,1] \times [0,1]$, где v — входное слово длины n, а w — соответствующее ему выходное слово, $n = 1, 2, \ldots$ (напомним, мы трактуем слово длины n в алфавите $\{0, 1, \ldots, p-1\}$ как число из $\{0, 1, \ldots, p^n - 1\}$). Множество $\mathcal{A}_{2\mathfrak{l}}$, стало быть, является измеримым относительно меры Лебега λ. Оказывается, что справедлив следующий *закон 0 или 1 для автоматов*: *для любого автомата* $\mathfrak{A}$, $\lambda(\mathcal{A}_{2\mathfrak{l}}) \in \{0, 1\}$. Отметим, что *если автомат* $\mathfrak{A}$ *конечен, то* $\lambda(\mathcal{A}_{2\mathfrak{l}}) = 0$; более того, $\lambda(\mathcal{A}_{2\mathfrak{l}}) = 1$ *тогда и только тогда, когда* $\mathfrak{A}$ *вполне транзитивен*. Мы доказываем, что *если детерминированная функция* f *отображает* $\mathbb{N}_0 = \{0, 1, 2, \ldots\}$ *в* $\mathbb{N}_0$, *а ее вторая производная* (*относительно* p*-адической метрики*) *отлична от нуля хотя бы в одной точке, причем* f *дифференцируема в окрестности этой точки, то соответствующий автомат абсолютно транзитивен*. Отсюда следует, например, что автомат, задающий полином над $\mathbb{Z}$ степени выше 1, а также автоматы, задающие функции $f(x) = x + (x^2 \mathbin{\mathsf{OR}} c)$ (где $c \in \mathbb{N}_0$), $f(x) = (1 + pz)^x$ (где $z \in \mathbb{N}_0 \setminus \{0\}$) абсолютно транзитивны.

Работа выполнена при поддержке РФФИ, проект 09-01-00653-а.

Список литературы

1. Anashin V., Khrennikov A. Applied algebraic dynamics. — Berlin—N.Y.: W. de Gruyter, 2009.

О ПРОБЛЕМЕ ПОЛНОТЫ В ИСЧИСЛЕНИИ ВЫСКАЗЫВАНИЙ

Г. В. Боков (Москва)

Рассматриваются тавтологии или тождественно истинные формулы над связками $\{\wedge, \vee, \neg, \to\}$. Множество всех тавтологий обозначим через T. Будем придерживаться стандартных соглашений по опусканию скобок [5]. Следующим не менее важным объектом исчисления высказываний выступают правила вывода, позволяющие из тавтологий снова получать тавтологии:

1) *Правило подстановки.* Пусть $\mathfrak{A}$ — тавтология, содержащая переменное высказывание X, а $\mathfrak{B}$ — произвольная формула над связками $\{\wedge, \vee, \neg, \to\}$. Тогда, если заменить в $\mathfrak{A}$ все вхождения X на $\mathfrak{B}$, то полученная формула также будет тавтологией.

2) *Правило заключения* или *modus ponens.* Если формулы $\mathfrak{A}$ и $\mathfrak{A} \to \mathfrak{B}$ — тавтологии, то формула $\mathfrak{B}$ также тавтология.

При рассмотрении алгебраических систем, частным случаем которых является исчисление высказываний, удобно ввести понятие оператора замыкания J, порожденного правилами вывода [2]. Пусть $M \subseteq T$, обозначим через $[M]$ множество всех тавтологий, которые либо принадлежат M, либо получены с помощью однократного применения правил вывода к тавтологиям, принадлежащим M. Определим множества $M_k \subseteq T$ индукцией по k:

$$M_0 = M, \ M_{k+1} = [M_k].$$

Тогда положим $J(M) = \bigcup\limits_{k=0}^{\infty} M_k$. Непосредственно из определения следует, что J является алгебраическим оператором замыкания, т. е. для любого $M \subseteq T$ и для любой формулы $\mathfrak{A} \in T$, если $\mathfrak{A} \in J(M)$, то $\mathfrak{A} \in J(M')$, где M' — конечное множество тавтологий из M.

Таким образом определенный оператор замыкания позволяет в его терминах сформулировать проблему полноты. Система тавтологий $M \subseteq T$ называется *полной* в T, если $J(M) = T$. Проблема полноты исчисления высказываний выглядит следующим образом: для произвольной системы тавтологий M из T требуется выяснить, является ли она полной в T или нет. Данная проблема эквивалентна задаче описания всех подмножеств M, которые являются полными в T, последняя является частным случаем решения проблемы выразимости. Скажем, что множество $M_2 \subseteq T$ *выразимо* через $M_1 \subseteq T$ с помощью оператора J, если $M_2 \subseteq J(M_1)$. Тогда проблема выразимости в терминах оператора J выглядит следующим образом: найти все такие пары (M_1, M_2), что $M_1, M_2 \subseteq T$ и $M_2 \subseteq J(M_1)$.

В качестве основного подхода к решению проблемы полноты используется подход, основанный на получении критериев полноты в терминах предполных классов. Принцип определения критериев зависит от свойств структуры замкнутых подмножеств рассматриваемого множества. В нашем случае произвольное подмножество тавтологий M будем называть *замкнутым* относительно оператора J, если $J(M) = M$. Для замкнутых относительно оператора J классов справедлива

Теорема. *Множество замкнутых классов имеет мощность континуума.*

Основным понятием в данном подходе служит понятие критериальной системы. Оно определяется следующим образом: пусть $\Delta(T)$ — совокупность всех замкнутых подмножеств множества T. Поскольку $J(T) = T$, то $\Delta(T)$ не пуст. *Критериальной системой* называется произвольное подмножество $\Theta, \Theta \subseteq \Delta(T)$, обладающее свойством: всякое множество M тавтологий из T является полным тогда и только тогда, когда для любого элемента $Q, Q \in \Theta$, выполнено соотношение $M \not\subseteq Q$. Критериальная система является *приведенной*, если она не содержит собственных критериальных подсистем. Замкнутый класс тавтологий M будем называть *предполным*, если $J(M) \neq T$ и, при добавлении к M любой тавтологии из $T \setminus M$, получается полная система.

Поскольку J — это алгебраический оператор и для исчисления высказываний существует конечная система аксиом, порождающая все тавтологии из T ([1] и [5]), то каждый замкнутый класс содержится в некотором предполном классе [2]. Согласно [3], это эквивалентно тому, что система предполных классов в T образует критериальную систему. Таким образом, проблема полноты для множества тавтологий из T свелась к рассмотрению множества всех предполных классов в T. Однако, следующая теорема показывает, что свойство критериальности множества предполных классов не дает эффективной процедуры решения проблемы полноты.

Теорема. *Множество предполных классов имеет мощность континуума.*

Важным частным случаем является рассмотрение не любых, а лишь конечных полных систем тавтологий. Следующая теорема дает возможность построить эффективную разрешающую процедуру для проблемы полноты таких систем.

Теорема. *Существует счетная система предполных классов, критериальная относительно проблемы полноты конечных систем тавтологий, и не существует конечной системы предполных классов, обладающих этим свойством.*

Как показывает следующая теорема для конечных систем тавтологий нельзя выбрать счетное критериальное множество предполных классов, для которого существовала бы эффективная процедура распознавания полноты конечных систем.

Теорема. *Свойство полноты конечных систем тавтологий алгоритмически неразрешимо.*

Из данной теоремы вытекает важное следствие, касающееся решения проблемы выразимости для исчисления высказываний.

Следствие. *Проблема выразимости для исчисления высказыва-*

ний алгоритмически неразрешима.

Список литературы

1. Колмогоров А. Н., Драгалин А. Г. Введение в математическую логику. — М.: Изд-во Моск. ун-та, 1982.

2. Кон П. Универсальная алгебра. — М.: Мир, 1968.

3. Кудрявцев В. Б. Функциональные системы. — М.: Изд-во Моск. ун-та, 1982.

4. Мальцев А. И. Алгоритмы и рекурсивные функции. — М.: Наука, 1965.

5. Новиков П. С. Элементы математической логики. — М.: Наука, 1973.

ОБ АСИМПТОТИЧЕСКОМ ПОВЕДЕНИИ ХРОМАТИЧЕСКОГО ИНДЕКСА СЛУЧАЙНЫХ ГИПЕРГРАФОВ

Ю. А. Будников (Москва)

Для формулировки основного результата необходимы следующие определения.

Упаковка в гиперграфе G — набор P непересекающихся ребер G, $\chi(G)$ — "хроматический индекс" графа G — минимальное число упаковок, на которые можно разбить все ребра G. Рассмотрим полный гипреграф $G(n) = (V(G(n)), E(G(n)))$ на n вершинах, k-однородный, т. е. любое его ребро $e \in E(G(n))$ содержит в точности k вершин из множества $V(G(n))$. Степень любой его вершины C_{n-1}^{k-1}, $|E(G(n))| = C_n^k$.

Введем вероятностное пространство $(\Omega, \mathcal{F}, \mathsf{P})$, где Ω — множество всех подмножеств $Z_i \in E(G), i = \overline{1, 2^{C_n^k}}$, $\mathcal{F}$ — множество всевозможных подмножеств Ω. Если происходит элементарный исход $Z_i = \{e_{i_1}, ..., e_{i_m}\}$, то говорим, что "родились ребра $e_{i_1}, ..., e_{i_m}$". Пусть все ребра рождаются независимо с вероятностью $p(n)$. На самом деле имеется в виду стандартная вероятностная модель испытаний Бернулли, где элементарные события — это кортежи из $0, 1$ длины C_n^k, где единицы на каких-то позициях соответствуют рожденным ребрам, а нули — не рожденным. На Ω вводится следующая вероятностная мера:

$$\mathsf{P}(Z_i) = \mathsf{P}(\text{родилось множество ребер } \{e_{i_1}, ..., e_{i_m}\} \text{ и не родились все оставшиеся ребра } G(n)) = p(n)^m (1 - p(n))^{c_n^k - m}.$$

На этом вероятностном пространстве определяется случайная величина $G(n,p) = Z_i$ с вероятностью $\mathsf{P}(Z_i)$. Это и есть случайный гиперграф, хроматический индекс которого оценивается в данной работе.

Пусть $p(n) = \frac{D(n)}{C_{n-1}^{k-1}}$, где $D(n)$ — возрастающая функция от n. Далее для краткости будем опускать аргумент у функций $D(n), p(n), k(n)$, если это не будет приводить к неоднозначной трактовке.

Далее везде c — произвольная константа, большая 1. Длина ребра гиперграфа $k(n)$ — функция от числа вершин гиперграфа n, возрастающая с ростом n в дискретном смысле. Упаковка в графе G — набор P непересекающихся ребер G. Покрытие графа G — набор K ребер графа, содержащий все вершины графа, $\chi(G)$ — "хроматический индекс" гиперграфа G — минимальное число упаковок, на которые можно разбить все ребра G.

Случайная упаковка — это упаковка в случайном гиперграфе $G(n,p)$. Она определяется следующим образом. Рассмотрим $P = \{e_{i_1}, ..., e_{i_s}\}$ — упаковка полного гиперграфа на n вершинах. Для каждого ее ребра $e_{i_j}, j = 1, ..., s$, на вероятностном пространстве Ω можно определить индикаторную случайную величину $I(e_{i_j}) = 1$ с вероятностью p, $I(e_{i_j}) = 0$ с вероятностью $1-p$. Если $I(e_{i_j}) = 1$, то говорим, что родилось ребро e_{i_j}, иначе говорим, что ребро e_{i_j} не родилось. По определению случайной упаковкой случайного гиперграфа $G(n,p)$ называется случайная величина $I(P) = \prod_{j=1}^{s} I(e_{i_j})$. Математическое ожидание числа родившихся упаковок равно

$$N(n) = \frac{n!}{(k!)^{\frac{n}{kc}}(n(1-\frac{1}{c}))!(\frac{n}{kc})!}\left(\frac{D}{C_{n-1}^{k-1}}\right)^{\frac{n}{kc}}.$$

Теорема 1. *Пусть $G(n,p(n))$ — случайный гиперграф $(n \to \infty)$:*

$$p(n) = \frac{D(n)}{C_{n-1}^{k(n)-1}} \le 1,\ k(n) = o(n),\ D(n) > c\left(\frac{n}{k(n)c}\right)^3\left(\frac{c}{c-1}\right)^{k(n)},$$

где $k(n)$ — возрастающая функция от n. Тогда для любого $\varepsilon > 0$ при $n \to \infty$ выполнено:

$$\mathsf{P}\left(\left|\frac{\sum_{P\in PG(n)} I(P)}{N(n)} - 1\right| > \varepsilon\right) < \frac{1}{\varepsilon^2}\left(\frac{1}{N(n)} + \frac{1}{\frac{n}{k(n)}\left(\frac{c}{c-1}\right)^{k(n)}}\right).$$

Теорема 2. *Пусть $G(n, p(n))$ — случайный гиперграф, $(n \to \infty)$:*

$$p(n) = \frac{D(n)}{C_{n-1}^{k(n)-1}} \leq 1,\ k(n) = o(n),\ D(n) > c\left(\frac{n}{k(n)c}\right)^3 \left(\frac{c}{c-1}\right)^{k(n)},$$

где $k(n)$ — возрастающая функция от n. Тогда для любого $\varepsilon > 0$ при $n \to \infty$ выполнено:

$$\mathsf{P}\left(\chi(G(n, p(n))) \leq [1 + \varepsilon + c\ln(k(n))]D(n)\right) \to 1.$$

Список литературы

1. Pippenger N., Spencer J. Asymptotic behavior of the chromatic index for hypergraphs // Journal of combinatorial theory. — 1989. — Series A, 51. — P. 24–42.

2. Будников Ю. А. Об асимптотическом поведении хроматического индекса случайных гиперграфов // Интеллектуальные системы. — 2007. — Т. 11. — С. 343–360.

3. Ширяев А. Н. Вероятность. 3-е изд. — М: МЦНМО, 2004.

КАК РОБОТАМ РЕШИТЬ ЗАДАЧУ О НАЗНАЧЕНИЯХ?

Н. О. Гаранина, Н. В. Шилов (Новосибирск)

Цель представленной работы — разработать мультиагентные алгоритмы для решения одной важной задачи [1] организации движения в мультиагентной системе, которая в классической теории может быть сведена к задаче о назначениях (наибольшем паросочетании минимального веса во взвешенном двудольном графе). Эта задача может быть названа задачей о роботах и укрытиях. В ней мультиагентная система состоит из n идентичных роботов, которым нужно "договориться" о выборе индивидуальных укрытий среди n возможных (число $n > 1$ роботов и укрытий одно и тоже). Предполагается, что каждый робот видит всех других роботов и все укрытия (ни какие три "объекта" системы не лежат на одной прямой). Задача системы в целом — самим роботам организовать посредством переговоров в парах выбор укрытия для каждого робота так, чтобы при прямолинейном движении к укрытиям у роботов

не произошло столкновений. В данном исследовании под мультиагентным алгоритмом мы будем понимать специальный класс распределенных алгоритмов [2], в котором каждое вычислительное устройство сети (т. е. агент) не является универсальным по Тьюрингу (способен выполнить очень ограниченный класс вычислений), но при этом является активным (может по своей инициативе предпринимать внешние дейсвия в системе, например, связываться с другим агентом), рациональным (предпринимает какие-либо действия исходя из соображений пользы для себя лично), а его внутренне состояние характеризуется терминах представлений агента о внешнем мире (belief), глобальных целей агента (desire) и сиюминутных намерений агента (intension); как известно, такие агенты называются BDI-агентами [3].

Для того, чтобы убедиться, что задача о роботах и укрытиях сводится к частному случаю задачи о назначениях, сформулируем следующую задачу комбинаторной геометрии, которую мы будем называть задачей Дейкстры [4, 5]: на плоскости n чёрных точек и n белых точек в общем положении (никакие три точки не лежат на одной прямой); необходимо соединить отрезками точки разного цвета так, чтобы эти отрезки не пересекались. Очевидно, что задача о роботах и укрытиях сводится к задачи Дейкстры; задача Дейкстры сводится уже к задачи о назначениях [4, 5]; хорошо известно, что задача о назначениях может быть решена централизовано (неким "диспетчером", управляющим всеми назначениями) за время $O(n^3)$ (например, венгерским алгоритмом).

Однако у задачи Дейкстры есть и другой вариант решения, предложенный самим Э. Дейкстрой [4, 5]: сначала строится произвольное соединение черных и белых точек; затем, пока в соединении есть пересекающиеся отрезки происходит "перещелкивание" какого-либо пересечения (произвольная пара пересекающихся отрезков $[B_1, W_1]$, $[B_2, W_2]$ заменяется на пару отрезков $[B_1, W_2]$ и $[B_2, W_1]$). Этот метод обязательно завершается, так как при перещелкивании сумма длин всех отрезков соединения убывает [4, 5]. Толчком к постановке задачи о роботах и укрытиях и исследованию мультиагентного алгоритма послужила интерпретация "перещелкивания" как локального разрешения конфликта между двумя роботами в результате переговоров.

Предположим, что каждый робот (агент) имеет специальную целочисленную переменную для хранения известного ему "числа конфликтов" (представляющую его belief). Цель каждого робота — выбрать укрытие, при движении к которому он не будет иметь стол-

кновений (это его desire). Работу каждого робота поделим на раунды, на каждом из которых этот робот должен ровно один раз поговорить со всеми другими роботами и, если нужно, сменить укрытие, к которому робот хочет идти (это его intention). Опишем алгоритм, как робот изменяет значение счетчика числа конфликтов и как ведет себя в зависимости от значения этого счетчика:

1) в начале каждого раунда робот устанавливает значение своего счетчика числа конфликтов $(n-1)$;

2) во время раунда при переговорах с очередным другим роботом (контрагентом на данный момент), робот проверяет, находится ли этот контрагент уже в укрытии или нет; если контрагент уже находится в укрытии, то робот уменьшает значение своего счетчика числа конфликтов на 1, завершает переговоры с этим контрагентом и переходит к переговорам со следующим роботом (если таковой имеется на данном раунде); если же контрагент не находится в укрытии, то:

2.1) робот вычисляет сумму S длин маршрутов этих двух роботов и сумму S' длин маршрутов, если эти роботы поменяются укрытиями (даже если маршруты не пересекаются);

2.) если S больше S', то робот обменивается укрытиями с контрагентом и заново устанавливает значение своего счетчика числа конфликтов в $(n-1)$;

2.3) если же S не больше S', то робот устанавливает значение свого счетчика числа конфликтов равным $(\max(m, m') - 1)$, где m и m' — соответственные числа конфликтов у самого робота и его контрагента;

2.4) робот завершает переговоры с этим контрагентом и переходит к переговорам со следующим роботом (если таковой имеется на данном раунде);

3) Если в конце раунда значение счетчика числа конфликтов у робота достигает 0, то робот "прыгает" (мгновенно переносится) в свое укрытие, а после этого только отвечает на запросы других роботов, что он уже находится в укрытии; в противном случае робот возвращается к пункту (1) алгоритма.

Теорема. *Если все роботы мультиагентной системы используют описанный алгоритм, а в начале работы системы все роботы имели разные укрытия, куда намеривались идти, то в системе не будет столкновений, а суммарное расстояние, которое пройдут роботы, будет оптимальным по Парето, а именно: если какой-либо робот решит выбрать для себя более короткий маршрут, то какому-то другому роботу обязательно придется выбрать более длинный маршрут.*

Таким образом можно считать, что мультиагентная задача о роботах и укрытиях решена (для прыгающих роботов). Это, однако, не означает, что найдено мультиагентное решение для задачи о назначениях или хотя бы задачи Дейкстры. Для задачи Дейкстры наш мультиагентный алгоритм для задачи о роботах и укрытиях попрежнему строит соединение с Парето-оптимальной суммой длин отрезков, но можно привести примеры, когда найденное этим алгоритмом соединение будет содержать пересекающиеся маршруты. Поэтому вопрос, поставленный в заглавии статьи остается открыты: как роботам решить задачу о назначениях (или хотя бы задачу Дейкстры)?

Работа выполнена в рамках интеграционногой программы СО РАН 2/12 "Формальные языки и методы спецификации, анализа и синтеза информационных систем". Авторы выражают признательность Л. А. Коняеву и Е. В. Бодину за обсуждение и ценные советы во время выполнения данного исследования.

Список литературы

1. Garanina N. O., Shilov N. V., Konyaev L.E. Can Robots Solve the Assignment Problem? // Proceedings of Workshop on Concurrency, Specification, and Programming CS&P 2009. — Warsow University. — V. 1. — P.154–163.

2. Тель Ж. Введение в распределенные алгоритмы. — М.: МЦНМО, 2009.

3. Wooldridge M. An Introduction to Multiagent Systems. — John Willey & Sons Ltd, 2002.

4. Андреева Т. В., Бодин Е. В., Городняя Л. В., Шилов Н. В. Этюд на тему Дейкстры: информатик в гостях у геометра // Потенциал. — 2006. — № 9. — С. 32–38.

5. Shilov N. V., Shilova S. O. Etude on theme of Dijkstra // ACM SIGACT News. — 2004. — 35 (3).

О ПРЕДИКАТНОЙ ЭКВИВАЛЕНТНОСТИ ФОРМУЛ АЛГЕБРЫ ЛОГИКИ

Э. Э. Гасанов, А. А. Шакиров (Москва)

Пусть R^2 — двумерное евклидово пространство и B^n — единичный n-мерный куб.

Пусть $X_1 \wedge X_2, X_1 \vee X_2, \neg X$ суть булевы функции, называемые, соответственно, *конъюнкцией, дизъюнкцией и отрицанием* и B — множество этих функций.

Обычным образом введем понятие формулы над B.

Две функции $F(X_1, \ldots, X_n)$ и $G(Y_1, \ldots, Y_m)$ из P_2 называются *равными*, если множества их существенных переменных совпадают и на любых двух наборах $\tilde{\alpha^n}$ и $\tilde{\beta^m}$, различающихся, может быть, только значениями несущественных переменных, выполнено

$$F(\tilde{\alpha^n}) = G(\tilde{\beta^m}).$$

Пусть Φ_B — множество всех формул над B и $\Phi_B(X_1, \ldots, X_n)$ (или просто $\Phi_B(n)$) — множество всех формул над B, реализующих функции, зависящие от переменных $X_1, \ldots, X_n$.

Формулы $\mathcal{A}$ и $\mathcal{B}$ из Φ_B называются *равными*, если они реализуют равные функции. Это отношение равенства разбивает Φ_B на классы эквивалентности $\mathcal{D}$, которые содержат точно все формулы, которые реализуют равные функции.

Открытое множество в R^2 будем называть *фигурой*. Пустое множество в R^2 будем называть пустой фигурой.

Рассмотрим множество базисных фигур в R^2 $\mathcal{G} = \{G_1, G_2, \ldots, G_n\}$. Каждой фигуре G_i сопоставим предикат $p_i(x_1, x_2)$, областью истинности которого является G_i, $i = 1, 2, \ldots, n$.

Пусть здесь и далее $\mathcal{P} = \{p_1(x_1, x_2), p_2(x_1, x_2), \ldots, p_n(x_1, x_2)\}$ и $\mathcal{A}(X_1, X_2, \ldots, X_n) \in \Phi_B(n)$. Подставим в $\mathcal{A}$ вместо каждой переменной X_i предикат p_i из $\mathcal{P}$. Данную операцию назовем *подстановкой*, и полученное выражение $\mathcal{A}(p_1, p_2, \ldots, p_n)$ назовем $\mathcal{P}$-*формулой*.

Поскольку описания фигуры G как в виде открытого подмножества плоскости, так и в виде предиката p, область истинности которого есть это подмножество G, являются тавтологичными, то мы далее будем использовать предикат p для обозначения фигуры G и будем говорить "фигура p" несмотря на то, что p — предикат, описывающий фигуру G.

Свяжем с каждой $\mathcal{P}$-формулой $\mathcal{A}(p_1, p_2, \ldots, p_n)$ некую фигуру $\mathcal{F}_{\mathcal{A}(p_1, p_2, \ldots, p_n)} \subseteq R^2$, которая описывается предикатом, задаваемым данной формулой (более подробно см. [1]).

Фигуры $\mathcal{F}_1$ и $\mathcal{F}_2$ называются *равными* (пишем $\mathcal{F}_1 = \mathcal{F}_2$), если они совпадают в R^2 как множества.

$\mathcal{P}$-формулы $\mathcal{A}(\mathcal{P})$ и $\mathcal{B}(\mathcal{P})$ назовем $\mathcal{P}$-*равными* (пишем $\mathcal{A}(\mathcal{P}) \overset{\mathcal{P}}{=} \mathcal{B}(\mathcal{P})$), если они задают равные фигуры.

Пусть здесь и далее $M = \{\pi_1, \ldots, \pi_k\}$ — некоторое подмножество множества всех n-подстановок Π^n.

Формулы $\mathcal{A}$ и $\mathcal{B}$ называются $(M, \mathcal{P})$-*равными,* (пишем $\mathcal{A} \overset{M,\mathcal{P}}{=} \mathcal{B}$), если при любой соответственно одинаковой подстановке $\pi \in M$ в них предикатов из $\mathcal{P}$ вместо переменных получаемые $\mathcal{P}$-формулы являются $\mathcal{P}$-равными.

Отношение $(M, \mathcal{P})$-равенства на множестве $\Phi_B(n)$ разбивает это множество на классы эквивалентности $\mathcal{D}_{M,\mathcal{P}}$, которые содержат точно все такие формулы, которые являются $(M, \mathcal{P})$-равными.

Будем говорить, что множество базисных фигур $\mathcal{P}$ обладает M-свойством, если отношения равенства булевских формул и $(M, \mathcal{P})$-равенства эквивалентны, т. е. разбиения $\mathcal{D}$ и $\mathcal{D}_{M,\mathcal{P}}$ совпадают, или, что то же самое, для любых двух формул $\mathcal{A}, \mathcal{B} \in \Phi_B(n)$ верно $\mathcal{A} \overset{M,\mathcal{P}}{=} \mathcal{B}$ тогда и только тогда, когда $\mathcal{A} = \mathcal{B}$.

Если p некоторая фигура, то функцию

$$h(p) = \begin{cases} 1, & \text{если } p \not\equiv 0 \\ 0, & \text{если } p \equiv 0 \end{cases}$$

назовем *предикатом пустоты* множества p.

Пусть p — некоторая фигура. Через p^1 обозначим фигуру p, а через p^0 — дополнение к фигуре p, т.е. фигуру $\overline{p}$. Пусть

$$\pi = \begin{pmatrix} 1 & 2 & \ldots & n \\ i_1 & i_2 & \ldots & i_n \end{pmatrix} —$$

n-подстановка из Π^n. Тогда булевскую функцию

$$\Omega_\pi^{\mathcal{P}}(\alpha_1, \ldots, \alpha_n) = h(p_{i_1}^{\alpha_1} \cap p_{i_2}^{\alpha_2} \cap \cdots \cap p_{i_n}^{\alpha_n})$$

назовем *определяющей функцией* множества базисных фигур $\mathcal{P}$ относительно подстановки π, а булевскую функцию

$$\chi_M^{\mathcal{P}} = \Omega_{\pi_1}^{\mathcal{P}} \vee \Omega_{\pi_2}^{\mathcal{P}} \vee \cdots \vee \Omega_{\pi_k}^{\mathcal{P}}$$

назовем *определяющей функцией* множества базисных фигур $\mathcal{P}$ относительно множества подстановок M.

Теорема. *Пусть* $M \subseteq \Pi^n$, *тогда множество базисных фигур* $\mathcal{P} = \{p_1, p_2, \ldots, p_n\}$ *обладает* M*-свойством тогда и только тогда, когда* $\chi_M^{\mathcal{P}} \equiv 1$.

Рассмотрим функции

$$k_i(t) = \left] \frac{n! - t + 1}{i!(n-i)!} \right[,$$

где $i \in \{1, 2, \ldots, n\}$, $]a[$ — наименьшее целое не меньшее чем a. Пусть ε — тождественная подстановка.

Теорема. *Для любых $n \in \mathbf{N}$, $t \in \{1, 2, \ldots, n!\}$, для любого множества $M \subseteq \Pi^n$, такого, что $|M| \geq t$, множество базисных фигур $\mathcal{P} = \{p_1, \ldots, p_n\}$ обладает M-свойством тогда и только тогда, когда на каждом слое i куба B^n существует хотя бы $k_i(t)$ наборов a_j таких, что $\Omega_\varepsilon^P(a_j) = 1$.*

Список литературы

1. Шакиров А. А. К логическому описанию геометрических фигур // Фундаментальная и прикладная математика. — 1999. — Т. 5, № 4. — С. 1191–1197.

РАСПОЗНАВАНИЕ ЛАБИРИНТНОСТИ ОТМЕЧЕННЫХ ГРАФОВ

В. И. Грунская (Ульяновск)

В настоящее время актуальны задачи, связанные с анализом различных сред с помощью блуждающих по ним агентов (мобильных роботов, автоматов, поисковых программ и т. п.). Агент перемещается по среде, получая при этом некоторую локальную информацию о ней, на основе которой, исходя из некоторой априорной информации, решает поставленные перед ним задачи: например, обходит среду и (или) делает заключения о ее свойствах. В таких задачах рассматриваются различные геометрические модели сред. Одной из них являются графы, которые можно рассматривать как топологическую модель среды [1]. В работе [2] описаны различные классы плоских лабиринтов, которые являются частным случаем как графовых, так и автоматных сред. В работах [3, 4] исследовались плоские ориентированные графы, и для них решались задачи, аналогичные классическим задачам теории автоматов: отличимости вершин и графов. Было показано, что длина различающего слова существенно зависит от того, расставлены ли отметки на дугах лабиринта в соответствии с их направлением или нет. То есть от того, является ли граф лабиринтом, или нет. В настоящем докладе предложен метод проверки "лабиринтности" графа.

Рассмотрим двумерное евклидово пространство с декартовой системой координат и целочисленную решетку Z^2 в нем. Элементы (x, y) множества Z^2 будем обозначать v. Расстоянием между $v = (x, y)$ и $v' = (x', y')$ будем называть число $\rho(v, v') = |x - x'| + |y - y'|$.

Элементы v и v' назовем соседними, если расстояние между ними равно единице.

Пусть $B = \{e, n, s, w\}$ — алфавит отметок дуг. Обозначим через b^{-1} отметку, противоположную к отметке b из B. Будем считать, что $e^{-1} = w$, $n^{-1} = s$, $w^{-1} = e$, $s^{-1} = n$. Обозначим через $A = 2^B \backslash \emptyset$.

Отмеченным графом $G = (V, E, a, b)$ назовем ориентированный конечный связный граф, у которого множество вершин V есть подмножество Z^2, E — множество дуг, $a : v \in V \to a \in A$ — функция разметки вершин, $b : (v, v') \in E \to b \in B$ — функция разметки дуг. Дуги (v, v') и (v', v) отмеченного графа назовем противоположными.

Симметрический планарный отмеченный граф назовем мозаичным, если он обладает следующими свойствами:

— дугами могут соединяться только соседние вершины;

— отметка каждой дуги естественным образом соответствует ее направлению;

— отметка вершины есть множество отметок всех исходящих из нее дуг.

Мозаичный граф назовем шахматным, если любые две его соседние вершины соединены парой противоположных дуг.

Отмеченные графы $G = (V, E, a, b)$ и $G' = (V', E', a', b')$ назовем изоморфными, если существует взаимно однозначное отображение множества V на множество V', сохраняющее смежность вершин и отметки вершин и дуг.

В докладе предложен метод проверки изоморфизма отмеченного графа G некоторому мозаичному графу. Для этого построена пара автоматов — исследователь и экспериментатор, аналогично тому, как это было сделано в [5]. Автомат-исследователь с красками обходит граф G. Он видит отметку и окраску вершины, в которой находится, отметки и окраску исходящих из нее дуг; может менять окраску вершины, в которой находится, и окраску исходящих из нее дуг; передавать информацию автомату-экспериментатору. Автомат-экспериментатор пытается восстановить плоскую укладку графа G, и, если граф планарен, проверяет полученную укладку на мозаичность и шахматность.

Список литературы

1. Kuipers B. The Spatial Semantic Hierarchy // Artificial Intelligence. — 2000. — V. 119, № 1–2. — P. 191–233.

2. Килибарда Г., Кудрявцев В. Б., Ушчумлич Щ. Независимые системы автоматов в лабиринтах //Дискретная математика. — 2003. — Т. 15, вып. 2. — С. 3–39.

3. Грунская В. И. Об отличимости плоских шахматных лабиринтов // Интеллектуальные системы. — 2004. — Т. 8. — С. 457–464.

4. Грунская В. И. Отличимость s-лабиринтов // Известия вузов. Математика. — 2009. — Т. 8. — С. 14–22.

5. Грунский В. И., Татаринов. Е. А. Распознавание графов при помощи блуждающего по ним агента // Проблемы теоретической кибернетики. Тезисы докладов XV международной конференции (Казань, 2–7 июня 2008г.) — Казань: Отечество, 2008. — С. 21.

МЕТОД ОЦЕНКИ СЛОЖНОСТИ И КЛАССИФИКАЦИИ ЗАКОНОВ ФУНКЦИОНИРОВАНИЯ ДИСКРЕТНЫХ ДЕТЕРМИНИРОВАННЫХ АВТОМАТОВ

А. С. Епифанов (Саратов)

Конечные детерминированные автоматы как математические модели сформировались для описания связей множеств сигналов и состояний с небольшим числом элементов. Это отражено в способах задания автоматов,основанных на явном указании функции (таблицы, конечные графы, матрицы, логические уравнения с переменными, заданными на конечных множествах). Функционирование автоматов базируется на рекурсии, которая позволяет представлять как угодно большой, но только начальный, фрагмент процесса функционирования. В работе [1] В. А. Твердохлебовым разработан новый подход для задания законов функционирования дискретных детерминированных динамических систем (автоматов),основанный на числовых структурах. Предложенный подход позволяет задавать законы функционирования геометрическими фигурами, которые в свою очередь могут быть заданы аналитически. Геометрический образ γ_s определяет полностью законы функционирования автомата A_s ,то есть всю фазовую картину связей входных последовательностей с выходными сигналами. Ввиду того, что геометрический образ законов функционирования автоматов при зафиксированных мощности входного алфавита X и линейном порядке на множестве $X*$ входных слов взаимно-однозначно определяется последовательностью вторых координат точек, свойства законов функционирования автоматов могут исследоваться на основе анализа свойств числовых последовательностей. В данной работе содержатся результаты исследований законов функционирования автоматов,

представленных в форме числовых последовательностей (последовательностей вторых координат точек геометрических образов) длиной до 5000000 знаков. Оценка сложности и классификация математических структур в форме последовательностей производится на основе спектра динамических параметров рекуррентного описания последовательностей [1]. Спектр $\Omega =< \Omega_0, \Omega_1, \Omega_2, \Omega_3, \Omega_4 >$ вводится как многоуровневая структура, в которой на каждом уровне представлены наборы характеристик использованных рекуррентных форм $F_i^m(z_1, z_2, ..., z_m) = z_{m+1}$, где m — порядок рекуррентной формы, $m = 1, 2, \ldots$. Полагается, что рекуррентная форма применяется отдельными вариантами вхождений рекуррентной формы в последовательность правил, определяющих рассматриваемую последовательность ξ. Данная работа является продолжением работ [2-3], в которых осуществлено построение и анализ классов автоматов, законы функционирования которых заданы в форме числовых последовательностей, и содержит результаты исследования свойств 10 распространенных фундаментальных математических величин: $\pi, e, \phi = \frac{1+\sqrt{5}}{2}$ (золотое сечение), $\sqrt{2}$, $\sqrt[3]{2}$, $\ln(2)$, $\ln(10)$, $\zeta(3) = \sum\limits_{x=1}^{\infty}(\frac{1}{x^3})$, константы Каталана C= $\sum\limits_{n=0}^{\infty}\frac{(-1^n)}{(2n+1)^2}$, константы Эйлера $\gamma = \lim\limits_{n\to\infty}(1 + \frac{1}{2} + \frac{1}{3} + ... + \frac{1}{n} - \ln(n))$. Анализируются начальные отрезки указанных последовательностей длины до 5000000 знаков. Обозначим указанное множество последовательностей длины 5000000 символом Υ. Проведенное исследование множества $\Upsilon = \{\upsilon_1, \upsilon_2, ..., \upsilon_{10}\}$ включило следующие этапы:

1. Построение на базе элементов множества Υ семи множеств последовательностей $\Psi_1, \Psi_2, \Psi_3, \Psi_4, \Psi_5, \Psi_6, \Psi_7$, каждое из которых состоит из 10000 последовательностей длины соответственно 50, 100, 200, 500, 1000, 2000 и 5000 знаков (построение множеств $\Psi_i, 1 \leq i \leq 7$ осуществляется на основе извлечения из каждой последовательности $\upsilon \in \Upsilon$ 1000 последовательностей длины $d_i, d_i \in \{50, 100, 200, 500, 1000, 2000, 5000\}$. Таким образом $\Psi_i = \psi_1^{d_i}, \psi_2^{d_i}, ..., \psi_{10000}^{d_i}$, где $\psi_j^{d_i} (1 \leq j \leq 10000)$ есть последовательность длины d_i извлеченная из $\upsilon_{[j/1000]}$ по следующему правилу:значением первого элемента последовательности $\psi_j^{d_i}$, $1 \leq j \leq 10000$ является значение элемента с номером $((j-1) \cdot d_i + 1)$ в последовательности $\upsilon_{[j/1000]}$, а значением последнего элемента последовательности $\psi_j^{d_i}$ является значение элемента с номером $(j \cdot d_i)$ в последовательности $\upsilon_{[j/1000]}$).

2. Построение спектров для элементов множеств $\Psi_1, \Psi_2, \Psi_3, \Psi_4, \Psi_5, \Psi_6, \Psi_7$.

3. Построение разбиений множеств $\Psi_i, 1 \leq i \leq 7$ на классы эквивалентных по сложности последовательностей по совпадению значений построенных спектров.

4. Вычисление среднего, минимального и максимального значения величины m_0 внутри каждого множества $\Psi_i, 1 \leq i \leq 7$, для каждого $\upsilon \in \Upsilon$.

В результате анализа полученных спектров не отмечено существенных скачков в распределении сложности на интервале до 5000000 знаков во всех 10 последовательностях множества Υ. Кроме того, средние значения показателя нулевого уровня Ω_0 спектра Ω внутри каждого множества $\Psi_i, 1 \leq i \leq 7$, для каждого $\upsilon \in \{\pi, e, \sqrt{2}, \sqrt[3]{2}, \ln(2), \ln(10), \zeta(3), C, \gamma\}$ отличаются только во втором знаке после запятой. Также отмечено еще одно свойство, которым обладают все элементы множества Υ — при увеличении длины извлекаемых последовательностей от 50 до 5000, значение показателя нулевого уровня спектра увеличивается лишь в 2 раза. В работах [2, 3] при анализе с использованием спектра Ω банка последовательностей OEIS отмечено, что резкое увеличение числа классов эквивалентных последовательностей происходит при переходе от разбиения P_0 (по показателям нулевого уровня спектра) к разбиению P_1(по показателям первого уровня спектра). Аналогичное свойство отмечено во всех построенных и проанализированных в данной работе множествах $\Psi_i, 1 \leq i \leq 7$, — число классов в P_1 больше, чем в P_0 примерно в 1000–1500 раз (увеличивается при увеличении длины последовательностей). Используемый аппарат геометрических образов законов функционирования автоматов [1] позволяет исследовать свойства законов функционирования дискретных детерминированных динамических систем на основе анализа свойств последовательностей из элементов конечного множества. В данной работе использование аппарата геометрических образов законов функционирования проиллюстрировано на фундаментальных математических последовательностях. Для оценки сложности и классификации использован спектр динамических параметров рекуррентного определения последовательностей. Построены и проанализированы спектры для 70000 последовательностей длины до 5000. Определены классы эквивалентных по сложности последовательностей и задаваемых ими законов функционирования дискретных детерминированных динамических систем.

Список литературы

1. Твердохлебов В. А. Геометрические образы законов функцио-

нирования автоматов. — Саратов: Научная книга, 2008.

2. Епифанов А. С. Анализ фазовых картин дискретных динамических систем. — Саратов: Научная книга, 2008.

3. Епифанов А. С. Анализ геометрических образов законов функционирования автоматов // Управление большими системами. Вып. 24. — М.: ИПУ РАН, 2009. — С. 81–98.

ПРЕДСТАВЛЕНИЕ КОЛЛЕКЦИЙ ЯЗЫКОВ АВТОМАТАМИ

М. А. Кибкало (Москва)

Определение сложности представления языков — одна из традиционных задач теории автоматов. В статье рассматривается случай совместной представимости семейства языков в одном автомате. Существуют различные определения сложности регулярного языка основанные на характеристиках самого языка или представляющего его автомата. В данной работе под сложностью языка (семейства непересекающихся конечных языков) понимается число состояний в представляющем его (их) приведенном автомате. В работе решена задача о нахождении точного значения максимальной сложности семейства конечных языков в зависимости от максимальной длины слова в нем.

Пусть A, B, Q — конечные алфавиты, $|A| = N, |B| = M$. Без ограничения общности можем считать, что $A = 0, 1, \ldots, N-1, B = 0, 1, \ldots, M-1$. Определим согласно [1] понятия конечного автомата (КА), инициального конечного автомата (ИКА), преставимости конечного языка в ИКА, регулярного языка.

Для $k \in Z_+$ определим классы языков $\mathbf{L_k}(A) = \{L \subseteq A^* \ | \forall \alpha \in L \Rightarrow |\alpha| = k\}$ и $\mathbf{L_{\leqslant k}}(A) = \{L \subseteq A^* \ | \forall \alpha \in L \Rightarrow |\alpha| \leqslant k\}$.

Пусть $L \subseteq A^*$ — любой регулярный язык, $s \geqslant 2$, $s \in N$. s-коллекцией языка L назовем семейство языков $\tau(L, s) = \{L_0, ..., L_{s-1}\}$ таких, что: $L_i \cap L_j = \varnothing$, $i \neq j$, $i, j = 0, ..., s-1$; $\bigcup_{i=1}^{s-1} L_i = L$; $L_0 \stackrel{def}{=} A^* \backslash L$.

Конечный инициальный автомат $V_{q_0} = (A, B, Q, \varphi, \psi, q_0)$ представляет s-коллекцию языка L $\tau(L, s)$ ($V_q \sim \tau(L, s)$) с помощью системы

подмножеств выходного алфавита $\{B_0, ..., B_{s-1}\}$,
$B_i \subset B,\ B_i \cap B_j = \varnothing,\ i \neq j,\ i,\ j = 0, ..., s-1$, если

$$\forall \alpha \in L_i \quad \psi(q_0, \alpha) \in B_i, \quad i = 0, ..., s-1.$$

Пусть $N \geqslant 2,\ M \geqslant 2,\ K \subseteq A^*$ — класс регулярных языков над алфавитом A. $c-$сложностью K назовем

$$S_{cc}(K, N, M) = \max_{L \in K} \max_{\tau(L,M)} \min_{V_q \sim \tau(L,M)} S_{ac}(V_q),$$

где $S_{ac}(V_q)$ — число состояний в автомате.

Теорема 1. $\forall N \geqslant 2,\ M \geqslant 2, \forall k \geqslant 1$ *существует* $p \geqslant 0$, *конечный язык* $L \in \mathbf{L_k}(A)$, *коллекция* $\tau(L, M)$ *и ИКА* $V_q(k, N, M) \sim \tau(L, M)$, *такие что*

$$S_{ac}(V_q(k, N, M)) = S_{cc}(\mathbf{L_k}(A), N, M) = \frac{N^{k-p} - 1}{N - 1} + \sum_{i=1}^{p} (M^{N^i} - p + 1).$$

Следствие 1. $\forall N \geqslant 2,\ M \geqslant 2$ *для* $S_{cc}(\mathbf{L_k}(A), N, M)$ *выполнено*

$$\frac{1}{N-1} \cdot \frac{N^k \cdot \log_N M}{k} \lesssim S_{cc}(\mathbf{L_k}(A), N, M) \lesssim \frac{N}{N-1} \cdot \frac{N^k \cdot \log_N M}{k}.$$

Теорема 2. $\forall N \geqslant 2,\ M \geqslant 2, \forall k \geqslant 1$ *существует* $p \geqslant 0$, *конечный язык* $L \in \mathbf{L}_{\leqslant \mathbf{k}}(A)$, *коллекция* $\tau(L, M)$ *и ИКА* $V_q(k, N, M) \sim \tau(L, M)$, *такие что*

$$S_{ac}(V_q(k, N, M)) = S_{cc}(\mathbf{L}_{\leqslant \mathbf{k}}(A), N, M) = \frac{N^{k-p} - 1}{N - 1} + M^{\frac{N^{p+1} - N}{N-1}}.$$

Следствие 2. $\forall N \geqslant 2,\ M \geqslant 2$ *для* $S_{cc}(\mathbf{L}_{\leqslant \mathbf{k}}(A), N, M)$ *выполнено*

$$\frac{N}{(N-1)^2} \cdot \frac{N^k \cdot \log_N M}{k} \lesssim S_{cc}(\mathbf{L}_{\leqslant \mathbf{k}}(A), N, M) \lesssim \frac{N^2}{(N-1)^2} \cdot \frac{N^k \cdot \log_N M}{k}.$$

Список литературы

1. Кудрявцев В. Б., Алёшин С. В., Подколзин А. С. Введение в теорию автоматов. — М.: Наука, 1985.

2. Кудрявцев В. Б., Подколзин А. С., Ушчумлич Ш. Введение в теорию абстрактных автоматов. — М.: Изд-во Моск. ун-та, 1985.

3. Campeanu C., Santean N., Yu S. Minimal cover-automata for finite languages // Proceedings of the Third International Workshop on Implementing Automata (WIA'98). — 1998. — P. 32–42.

О ПОСТРОЕНИИ ПРАВИЛЬНЫХ СЕМЕЙСТВ В НЕКОТОРЫХ КЛАССАХ ФУНКЦИЙ

О. В. Кондратьева (Москва)

Правильные семейства функций были введены в работе [1] для построения параметрических семейств латинских квадратов, которые широко используются в кодировании, шифровании и планировании эксперимента. На практике обычно применяются квадраты достаточно больших размеров. При этом их удобно задавать с помощью функции, которая определяет элемент квадрата по номеру строки и столбца. Именно при таком аналитическом методе задания латинского квадрата и используются правильные семейства функций.

Напомним необходимые определения. *Латинским квадратом* порядка n называется матрица размера $n \times n$, заполненная элементами некоторого n-элементного множества Ω таким образом, что в каждой ее строке и в каждом столбце все элементы различны.

Функции $f_1, f_2, \ldots, f_n$ от переменных $p_1, p_2, \ldots, p_n$ образуют *правильное семейство*, если для любых различных наборов $p' = (p'_1, p'_2, \ldots, p'_n)$ и $p'' = (p''_1, p''_2, \ldots, p''_n)$ найдется индекс α, $1 \le \alpha \le n$, такой, что $p'_\alpha \ne p''_\alpha$ и $f_\alpha(p') = f_\alpha(p'')$.

Графом существенной зависимости семейства функций $F = \{f_i\}_{i=1}^n$, $f_i = f_i(z_1, \ldots, z_n)$, называется ориентированный граф $G_F = (V, E)$ на множестве вершин $V = \{1, 2, \ldots, n\}$ такой, что $(i, j) \in E$, если и только если f_j существенно зависит от x_i.

В работе [2] доказана

Теорема. *Пусть $G(V, E)$ — произвольный ориентированный граф без петель и кратных ребер на n вершинах $V = \{1, 2, \ldots, n\}$. Тогда существует граф $G'(V', E')$ на $n' \le n + \lceil \log_2 n \rceil$ вершинах $V' = \{1, 2, \ldots, n\}$, реализуемый в виде графа существенной зависимости некоторого правильного семейства функций и такой, что его вершинный подграф на подмножестве $V \subseteq V'$ совпадает с G. Более того, для любого семейства функций $F = \{f_i\}_{i=1}^n$, реализующего исходный граф G, найдется правильное семейство функций $F' = \{f'_i\}_{i=1}^{n'}$, реализующее граф G' и такое, что для каждого i,*

$1 \le i \le n$, *существует набор значений аргументов* $x_{n+1}, \ldots, x_{n'}$, *при которых* f_i' *как функция от* n *аргументов* $x_1, \ldots, x_n$ *совпадает с* f_i.

На самом деле оценка числа вершин графа G' в данной теореме непонижаема: можно показать достижимость оценки числа вершин, которые необходимо добавить для того, чтобы из графа существенной зависимости произвольного семейства функций получить новый граф, являющийся графом существенной зависимости некоторого правильного семейства функций. При этом функции получаемого правильного семейства наследуют свойства семейства функций, реализующего исходный граф. Сформулируем это в виде теоремы.

Теорема. *Для любого* $n \ge 3$ *существует семейство функций* $F = \{f_i\}_{i=1}^n$, $f_i = f_i(z_1, \ldots, z_n)$, *к графу существенной зависимости которого необходимо добавить ровно* $\lceil \log_2 n \rceil$ *вершин для того, чтобы получить граф* G', *являющийся графом существенной зависимости некоторого правильного семейства функций* F'. *При этом семейство* F' *можно выбрать так, что для каждого* i, $1 \le i \le n$, *существует набор значений аргументов* $x_{n+1}, \ldots, x_{n'}$, *при которых* f_i' *как функция от* n *аргументов* $x_1, \ldots, x_n$ *совпадает с* f_i.

Примером такого семейства может служить следующее:

$f_1 = x_2 x_3 \cdot \ldots \cdot x_n$

$f_2 = x_1 x_3 \cdot \ldots \cdot x_n$

$\vdots$

$f_n = x_1 x_2 \cdot \ldots \cdot x_{n-1}$.

Более того, ни для одного из предполных классов в P_2 данная оценка неулучшаема.

Теорема. *Пусть* $n \ge 3$ *и* R — *любой из предполных классов в* P_2 *(т.е. любой из классов* T_0, T_1, L, M, S*).*

Существует семейство функций $F = \{f_i\}_{i=1}^n$, $f_i \in R$, *к графу существенной зависимости которого необходимо добавить ровно* $\lceil \log_2 n \rceil$ *вершин, чтобы полученный граф реализовывался как граф существенной зависимости некоторого правильного семейства функций.*

Например, для классов T_0, T_1, M можно рассмотреть семейство, указанное выше, а для класса линейных функций — семейство

$f_1 = x_2 + x_3 + \ldots + x_n$

$f_2 = x_1 + x_3 + \ldots + x_n$

$\vdots$

$f_n = x_1 + x_2 \ldots + x_{n-1}$.

Список литературы

1. Носов В. А. О построении классов латинских квадратов в булевой базе данных // Интеллектуальные системы. — 1990. — Т. 4, вып. 3–4. — С. 307–320.

2. Козлов А. А., Носов В. А., Панкратьев А. Е. Матрицы и графы существенной зависимости правильных семейств функций // Фундаментальная и прикладная математика. — 2008. — Т. 14, № 4. — С. 137–149.

ОЦЕНКИ ЧИСЛА ШАГОВ РАБОТЫ АЛГОРИТМОВ РЕШЕНИЯ ЗАДАЧ РАСПОЗНАВАНИЯ ОБРАЗОВ ПРИ ЛОГИКО-ПРЕДМЕТНОМ ПОДХОДЕ

Т. М. Косовская (Санкт-Петербург)

Рассматриваются задачи распознавания образов в следующей постановке [1]. *Распознаваемый объект* ω представлен как конечное множество $\omega = \{\omega_1, \ldots, \omega_t\}$. На частях распознаваемых объектов задан набор предикатов $p_1, \ldots, p_n$, характеризующих свойства и отношения между элементами *Описанием* $S(\omega)$ *объекта* ω называется набор всех истинных постоянных формул вида $p_i(\overline{\tau})$ или $\neg p_i(\overline{\tau})$, выписанных для всех возможных частей τ объекта ω. Множество всех распознаваемых объектов Ω разбито на K классов $\Omega = \bigcup_{k=1}^{K} \Omega_k$. *Описанием класса* Ω_k называется такая формула $A_k(\overline{x})$ со свободными переменными $\overline{x}$, что если для некоторого списка $\overline{\omega}$ всех элементов множества ω истинна формула $A_k(\overline{\omega})$, то $\omega \in \Omega_k$, представленная в виде дизъюнкции элементарных конъюнкций.

Решение задач идентификации, классификации, и анализа сложного объекта сведено в [1] к доказательству соответственно секвенций $S(\omega) \models \exists \overline{y}_{\neq} A_k(\overline{y})$, $S(\omega) \models \bigvee_{k=1}^{K} A_k(\overline{\omega})$, $S(\omega) \models \bigvee_{k=1}^{K} \exists \overline{y}_{\neq} A_k(\overline{y})$.

В [2] доказаны следующие теоремы.

Теорема 1. *Задачи идентификации, классификации и анализа сложного объекта NP-трудны.*

Теорема 2. *Если* m *— максимальное количество переменных в элементарных конъюнкциях, входящих в описания классов, то при использовании алгоритма полного перебора число шагов решения любой из сформулированных выше задач распознавания образов составляет* $O(t^m \cdot |A| \cdot |S|)$.

Теорема 3. *Если* $\widetilde{a}$ *— максимальное количество вхождений атомарных формул в элементарные конъюнкции, составляющие описания классов,* s *— максимальное количество вхождений одного и того же предиката (только без отрицаний или только с отрицаниями) в описание объекта,* D *— количество дизъюнктов в описаниях классов, используемых при решении задачи, то при использовании секвенциального исчисления предикатов или метода резолюций для исчисления предикатов число шагов решения любой из сформулированных выше задач распознавания образов составляет* $O(D \cdot s^{\widetilde{a}})$.

Для сокращения числа шагов решения поставленных задач в введено понятие многоуровневого описания классов, заключающееся в выделении подформул описаний классов и заменой их на атомарные формулы с новыми предикатами и переменными.

Пусть $P_i^l(\overline{y}_i^l)$ — подформулы формул $A_k^{l-1}(\overline{x}^{l-1})$, p_i^l и x_i^l — новые предикаты и переменные, определяемые равносильностями $p_i^l(x_i^l) \Leftrightarrow P_i^l(\overline{y}_i^l)$, $A_k^l(\overline{x}^l)$ получается из $A_k^{l-1}(\overline{x}^{l-1})$ заменой $P_i^l(\overline{y}_i^l)$ на $p_i^l(x_i^l)$ $(i = 1,...,n_l,\ l = 1,...L)$. В [3] доказаны оценки числа шагов решения сформулированных задач, в частности, доказана теорема.

Теорема 4. *Для того, чтобы при использовании двухуровневого описания классов число шагов работы переборного алгоритма, решающего задачу анализа сложного объекта, уменьшилось по сравнению с исходным (начиная с некоторого* t*), достаточно чтобы* $|S| \cdot (\sum_{k=1}^{K} t^{m_k} \cdot |A_k| - \sum_{j=1}^{n_1} t^{\mu_j^1} \cdot |P_j|) \geq |S^1| \cdot \sum_{k=1}^{K} {t_1}^{\delta_k^1 + n_k^1} \cdot |A_k^1|$, *где* $|S|$ *и* $|S^1|$ *— длины записи исходного описания объекта и его описания в терминах предикатов первого уровня,* $|A_k|$, $|A_k^1|$ *и* $|P_j|$ *— длины записи исходных описаний классов, их описаний в терминах предикатов первого уровня и формул, определяющих предикаты первого уровня,* m_k, μ_j^1 *и* $\delta_k^1 + n_k^1$ *— количество аргументов у формул* $A_k(\overline{x})$, $P_i^1(\overline{y}_i^1)$ *и* $A_k^1(\overline{x}^1)$ *соответственно.*

Для решения задач распознавания объекта в условиях неполной информации и распознавания частично заслоненного объекта вводится понятие неполного вывода для элементарной конъюнкции, заключающийся в том, что из заданного множества постоянных формул следует не сама элементарная конъюнкция, а лишь некоторая ее подформула, причем нет информации о том, что исходная формула противоречит заданному множеству постоянных формул. В [4] доказаны теоремы.

Теорема 5. *Число шагов работы переборного алгоритма проверки неполной выводимости секвенции* $S(\omega) \vdash \exists \overline{x}_{\neq}\ A(\overline{x})$ *составляет* $O(t^m \cdot 2^{a-1})$, *где* t *— число объектов предметной области,*

m — число предметных переменных в формуле $A(\overline{x})$, a — количество атомарных формул в $A(\overline{x})$.

Теорема 6. *Число шагов работы алгоритма проверки неполной выводимости секвенции $S(\omega) \vdash \exists \overline{x}_{\neq}\ A(\overline{x})$ в секвенциальном исчислении предикатов составляет $O(s^{a-1} \cdot a^2 \cdot (s + \eta^2 \cdot a))$, если $s \geq 2$, где s — наибольшее число вхождений каждого из предикатов p_i в множество $S(\omega)$, a — количество атомарных формул в $A(\overline{x})$, η — максимальное количество аргументов предикатов p_1,...,p_n.*

Для группы преобразований, действующих на распознаваемые объекты, G^* с конечным числом образующих $G = \{g_1, ..., g_T\}$ вводится понятие *описания преобразования* g_j (множество которых обозначается посредством $\Gamma_j^l(\overline{x})$) вида $B_j^l(\overline{x}) \Leftrightarrow C_j^l(\overline{g_j(x)})$, где $B_j^l(\overline{x})$ и $C_j^l(\overline{g_j(x)})$ — элементарные конъюнкции.

Решение задач инвариантной идентификации, инвариантной классификации и инвариантного анализа сложного объекта в [5] сведены к доказательству соответственно формул $S(\omega)\ \Gamma(\overline{x}) \models \exists \overline{y}_{\neq} A_k(\overline{y})$, $S(\omega)\ \Gamma(\overline{x}) \models \bigvee_{k=1}^{K} A_k(\overline{\omega})$, $S(\omega)\ \Gamma(\overline{x}) \models \bigvee_{k=1}^{K} \exists \overline{y}_{\neq} A_k(\overline{y})$.

Теорема 7. *Число шагов инвариантной идентификации класса, замкнутого относительно группы G^* с конечным числом образующих $G = \{g_1, ..., g_T\}$ при ограничении, что глубина вложенности термов, задающих преобразования из группы G^*, не превосходит заданного числа R, составляет $O(T^R \cdot R \cdot |S| \cdot (t^{m_k} \cdot |A_k| + t^{m^c} \cdot |C| \cdot L) + \Delta \cdot T^{R-1} \cdot R^2 \cdot (t^{m_k} \cdot |A_k| + t^{m^c} \cdot |C| \cdot L))$ при использовании алгоритма полного перебора или $O(T^R \cdot (J_k \cdot (s + R \cdot \delta)^{\widetilde{a}} + (s + R \cdot \delta)^c)$, если использован алгоритм поиска вывода в исчислении предикатов.*

Список литературы

1. Косовская Т. М., Тимофеев А. В. Об одном новом подходе к формированию логических решающих правил // Вестник ЛГУ. — 1985. — № 8. — С. 22–27.

2. Косовская Т. М. Доказательства оценок числа шагов решения некоторых задач распознавания образов, имеющих логические описания // Вестн. С.-Петербург. ун-та. Сер. 1. Математика, механика, астрономия. — 2007. — Вып. 4. — С. 82–90.

3. Косовская Т. М. Многоуровневые описания классов для уменьшения числа шагов решения задач распознавания образов, описываемых формулами исчисления предикатов // Вестн. С.-Петербург. ун-та. Сер. 10. — 2008. — Вып. 1. — С. 64–72.

4. Косовская Т. М. Частичная выводимость предикатных формул как средство распознавания объектов с неполной информацией //

Вестн. С.-Петерб. ун-та. Сер. 10. — 2009. — Вып. 1. — С. 74–84.

5. Косовская Т. М. Распознавание объектов из классов, замкнутых относительно группы преобразований // Вестн. С.-Петерб. ун-та. Сер. 10. — 2009. — Вып. 3. — С. 45–55.

СЛОЖНОСТЬ РАСПОЗНАВАНИЯ ТРАССИРОВАНИЙ АБСТРАКТНЫХ ЗНАНИЙ

К. И. Костенко (Краснодар)

Пространства знаний это специальный тип интеллектуальных систем, представляющих целостные семейства знаний произвольных предметных областей. Абстрактные пространства знаний являются формальной моделью пространств знаний, представленной алгебраическими системами четырёх специальных типов [1]. К ним относятся пространства конфигураций, порождаемые множествами идеализированных знаний. Конфигурации представляются нагруженными бинарными деревьями, в которых висячим вершинам сопоставляются элементарные (неделимые) конфигурации, а внутренним вершинам — семантические отношения, выполняющимися между конфигурациями, представленными левыми и правыми поддеревьями соответствующих вершин. Трассируемость конфигураций определяется существованием отображений структуры одной конфигурации в структуру другой конфигурации, для которого разметки сопоставляемых вершин оказываются сравнимыми [1]. Трассирования лежат в основе уточнений теоретически и практически важных свойств формализованных знаний. Возможность практического применения трассирований определяется сложностью алгоритмов ее распознавания.

Структурное представление конфигураций. Пусть M — носитель пространства конфигураций, представляющий бесконечное аычислимое множество, содержащее пустую конфигурацию Λ, а R — вычислимое множество разрешимых бинарных отношений на M, на котором задано разрешимое отношение вложения ρ_1. Разложением конфигураций называется всюду определенное вычислимое отображение $\epsilon : M \times M \mapsto M$, для которого:

$\epsilon(\Lambda) = (\Lambda, \Lambda)$ и $\forall\, z_1, z_2 \in M\, \exists\, z \in M\, (\epsilon(z) = (z_1, z_2))$.

Конфигурация $z \in M$ называется элементарной, если $\epsilon(z) = (\Lambda, \Lambda)$. Пусть M_0 и M_1 множества элементарных (неэлементарных) конфигураций в разложении ϵ. На множестве M_0 определим разрешимое отношение порядка ρ_0.

Вычислимое отображение $\psi : M_1 \to R$ называется семантическим связыванием для разложения ϵ, если:

1) $\forall\, z \in M_1\, (\epsilon(z) \in \psi(z))$;

2) $\forall\, z_1, z_2 \in M\, \forall\, r \in R((z_1, z_2) \in r \to \exists z \in M(\epsilon(z) = (z_1, z_2) \wedge \psi(z) = r))$.

3) ψ является инъективным на множествах конфигураций, имеющих одинаковые разложения.

Пространством конфигураций называется алгебраическая система с носителем $M \cup R$, для которой задана операция декомпозиции $d = (\epsilon, \psi)$, где ϵ — разложение, а ψ — семантическое связывание для ϵ.

Конфигурациям соответствуют их полные структурные представления (ПСП). Корню ПСП $z \in M_1$, приписывается отношение $\psi(z)$, а его левое и правое поддерево представляют ПСП конфигураций из $\epsilon(z)$. ПСП конфигураций из M_0 — одновершинные и размечены этими конфигурациями. Разложение ϵ называется конечным если ПСП всех конфигураций — конечные.

Трассирования конфигураций. Будем кодировать вершины бесконечного насыщенного бинарного дерева элементами множества конечных двоичных последовательностей I. Пусть $z \in M$. Множество вершин (висячих вершин) ПСП z обозначим как $D(z)$ $(O(z))$.

Изотонное отображение $\xi : I \to I$: называется трассированием $z_1 \in M$ в $z_2 \in M$, если:

1) $\xi(D(z_1)) \subseteq \xi(D(z_2)) \wedge \forall \alpha \in D(z_1)(\alpha \in D(z_1) \setminus O(z_1) \leftrightarrow \xi(\alpha) \in D(z_2) \setminus O(z_2))$;

2) $\forall\, \alpha, \alpha\sigma \in D(z_1), \sigma \in \{0,1\}\ \exists\ \beta, \gamma \in I\ ((\xi(\alpha) \subset \xi(\alpha\sigma) \to \xi(\alpha\sigma) = \xi(\alpha)\beta\sigma\gamma)$

Отображения трассирования конфигураций с дополнительными условиями на β и γ определяют классы, c-трассирований (β и γ — пустые) и o-трассирований (β — пустое). Инъективные трассирования называются p-трассированиями [1]. Сложность алгоритмов распознавания трассируемости конфигураций определяется числом сравнений в ρ_1 и ρ_2.

Теорема 1. *Вычислительная сложность распознавания c-трассируемости конфигураций не превосходит n^2.*

Алгоритм распознавания c-трассируемости $z_1 \in M$ в $z_2 \in M$, сложность которого равна n^2, использует обход ПСП z_1 в глубину сверху вниз [2]. Он проверяет возможность определения отображения c-трассирования ξ, для которого в качестве значений ξ выбираются элементы $D(z_2)$ также проходимого в глубину. При этом используются следующие свойства c-трассирования ξ конфигурации

z_1 в z_2: 1) ξ отображает самую левую ветвь $D(z_1)$ на самую левую ветвь $D(z_2)$; 2) множество вершин из $D(z_1)$, отображаемых ξ в вершину $D(z_2)$, образуют семейство деревьев; 3) если $\xi(\beta) = \alpha$, где $\beta = \sigma_1, ..., \sigma_k$, $\alpha = \delta_1, ..., \delta_q$, то последовательность слов, являющихся началами β, сопоставляется всем началам α.

Обход ПСП z_1 разбивается на этапы прохождения по ветвям, образованным левыми потомками последовательно выбираемых вершин в ПСП z_1. Этапы реализуются в начале обхода, а также после всякого перехода к правым потомкам вершин.

Теорема 2. *Вычислительная сложность распознавания p-трассируемости конфигураций не превосходит* n^2.

Алгоритм построения инъективных трассирований произвольных конфигураций z_1 и z_2 указанний сложности основан на обходе ПСП z_1 в глубину. В качестве значений ξ выбираются вершины ПСП z_2 также в порядке обхода дерева $D(z_2)$ в глубину. В процессе построения ξ формируется список L_1, образованный такими парами (α, β), что не существует p-трассирования z_1 в z_2, для которого $\xi(\alpha) = \beta$. Если для вершин α и β будет найдено p-трассирование $(z_1)_\alpha$ в $(z_2)_\beta$, для которого $\xi(\alpha) = \beta$, то включим пару (α, β) в список L_2. Это позволяет избежать поиска p-трассирований подконфигураций z_1 в те подкон фигурации z_2, для которых их отсутствие (существование) уже установлено.

Список литературы

1. Костенко К. И. Компоненты и операции абстрактных пространств знаний // Материалы Всероссийской конференции ЗОНТ09 (20–22 октября 2009 г.). Т. 2. — С. 36–40.

2. Ахо А., Хопкрофт Д., Ульман Д. Структуры данных и алгоритмы. — Вильямс, 2003.

О РАСПОЗНАВАНИИ СВОЙСТВА ОБРАТИМОСТИ ДЛЯ МОНОФУНКЦИОНАЛЬНЫХ КЛАССОВ БИНАРНЫХ КЛЕТОЧНЫХ АВТОМАТОВ

И. В. Кучеренко (Москва)

Клеточные автоматы (КА) являются дискретной математической моделью процессов, для которых существенна не только временная, но и пространственная протяженность [1]. Обратимые клеточные автоматы — это собственный подкласс в классе всех КА,

характеризующийся тем, что в процессе функционирования КА из этого класса не происходит потери информации. Класс обратимых КА представляет как теоретический интерес (модели "обратимой вселенной"), так и практический — в связи с задачами защиты информации, синтеза квантовых вычислителей, проектирования чипов с пониженным энергопотреблением и других.

В работе пойдет речь о задаче алгоритмического распознавания свойства обратимости в классах двумерных бинарных КА (у которых ячейка имеет два состояния). Автором установлено, что свойство обратимости не распознаваемо в классе всех двумерных бинарных клеточных автоматов [2]. С другой стороны, в классе двумерных бинарных клеточных автоматов, в которых содержатся только КА с линейными локальными функциями переходов, свойство обратимости разрешимо [3]. В связи с этим возникает задача классификации "естественных" классов КА на те, в которых свойство обратимости разрешимо, и те, для которых это не так.

В работе рассматриваются классы бинарных двумерных КА, имеющих фиксированную локальную функцию переходов (в таком классе варьируются исключительно вектора в локальном шаблоне соседства); такие классы будем называть монофункциональными. Автором установлено, что существуют монофункциональные классы с неразрешимым свойством обратимости.

Приведем необходимые для понимания полученного результата определения. Формально клеточный автомат σ представляет из себя четверку вида (Z^k, E_n, V, φ), где Z^k — совокупность всех k-мерных векторов с целочисленными координатами, E_n — конечное множество из n элементов, природа которых не существенна. Для простоты их можно считать числами из множества $\{0, 1, \ldots, n-1\}$. $V = \{v_1, v_2, \ldots, v_m\}$ — упорядоченный набор различных ненулевых векторов из Z^k. $\varphi : (E_n)^{m+1} \mapsto E_n$, $\varphi(0, 0, \ldots, 0) = 0$. Элементы множества Z^k называются ячейками, E_n — состояниями ячеек, 0 — состояние покоя. При помощи шаблона соседства V каждой ячейке α ставится в соответствие набор векторов $V(\alpha) = \{\alpha, \alpha + v_1, \alpha + v_2, \ldots, \alpha + v_m\}$, который называется ее окрестностью. Функция φ называется локальной функцией переходов клеточного автомата.

Функции $g : Z^k \mapsto E_n$ называются состояниями КА. Основная функция переходов Φ задается как отображение множества всех состояний клеточного автомата σ в себя, причем если $g = \Phi(g')$, то $g(\alpha) = \varphi(g'(\alpha), g'(\alpha + v_1), g'(\alpha + v_2), \ldots, g'(\alpha + v_m)), \forall\alpha$. Функционирование КА определяется как последовательность его состо-

яний $g_0, g_1, g_2, \ldots$, получающаяся в результате применения основной функции переходов к некоторому его состоянию g_0, то есть $g_t = \Phi(g_{t-1}) = \Phi^t(g_0)$, t — натуральное число. Состояние клеточного автомата, в котором только конечное число ячеек находится в ненулевом состоянии, называется конфигурацией.

Клеточный автомат, основная функция переходов которого инъективна на множестве всех конфигураций, называется обратимым. По теореме Мура—Майхилла [1] множество обратимых клеточных автоматов совпадает с множеством КА, основная функция переходов которых является сюръективной.

Пусть φ — булева функция, зависящая от $m+1$ переменных и сохраняющая ноль. Множество двумерных клеточных автоматов с локальной функцией переходов φ обозначим через $CA(2, 2, m, \varphi)$. Будем задавать индивидуальные клеточные автоматы из множества $CA(2, 2, m, \varphi)$ набором из m двумерных ненулевых целочисленных векторов V (их шаблоном соседства). Задача алгоритмического распознавания свойства обратимости заключается в построении машины Тьюринга, которая на наборе $V = ((x_1, y_1), (x_2, y_2), \ldots (x_m, y_m))$, записанному на ее ленте в виде последовательности из $2 \cdot m$ натуральных чисел $x_1, y_1, x_2, y_2, \ldots, x_m, y_m$ в унитарной записи (отдельные числа разделяются одиночной буквой "0"; в начальном состоянии на всей "свободной" части ленты записана буква "0", головка находится над самой левой буквой "1" конфигурации), останавливалась, при этом в ячейке ленты, находящейся под головкой в момент остановки, должно находиться буква "1", если клеточный автомат $\sigma = (Z^2, E_2, V, \varphi)$ обратим, или "0", если σ не обратим.

Теорема 1. *Существует самодвойственная сохраняющая ноль булева функция $\varphi(x_0, x_1, \ldots, x_m)$, такая, что в классе $CA(2, 2, m, \varphi)$ свойство обратимости алгоритмически не разрешимо.*

Автор выражает благодарность своему научному руководителю В. Б. Кудрявцеву за постановку задачи и внимание к работе.

Работа выполнена при поддержке РФФИ, проект 06–01–00240.

Список литературы

1. Кудрявцев В. Б., Подколзин А. С., Болотов А. А. Основы теории однородных структур. — М.: Наука, 1990.

2. Кучеренко И. В. О разрешимости обратимости клеточных автоматов // Интеллектуальные системы. — 2004. — Т. 8, вып. 1–4. — С. 465–482.

3. Кучеренко И. В. О структуризации класса обратимых бинарных клеточных автоматов // Интеллектуальные системы. — 2005. — Т. 9, вып. 1–4. — С. 445–456.

АСИМПТОТИКА ПРОМЕЖУТОЧНЫХ ФУНКЦИЙ РОСТА СЛОЖНОСТИ ПОИСКА ДЛЯ СЛУЧАЙНЫХ БАЗ ДАННЫХ

Н. С. Кучеренко (Москва)

Теория хранения и поиска информации является важным разделом теории интеллектуальных систем. Одним из ключевых объектов этой теории является информационный граф (ИГ) [1] — управляющая система, которая позволяет рассматривать имеющиеся модели данных и задачи, связанные с ними, с более общих позиций.

В работе рассматривается задача поиска на интервале $(0,1)$. Практически такая задача возникает, когда на объектах базы данных введен линейный порядок. Предполагается, что объекты рассортированы в соответствии с этим порядком, и по пришедшему запросу необходимо найти соответствующий ему объект базы данных. Алгоритмы поиска, использующие только операции сравнения, исследуются с точки зрения сложности, которая характеризует среднее время работы алгоритма.

Алгоритмы поиска представляются с помощью информационных графов (ИГ). Для любой задачи поиска существует оптимальный ИГ [2], сложность задачи поиска полагаем равной сложности такого ИГ. В зависимости от конкретной задачи поиска сложность оптимального ИГ может быть как логарифмом от мощности базы данных, так и константой. Автором исследуется вопрос о поведении сложности оптимального информационного графа на классах задач в среднем. Классы задач $\Upsilon_n(f,g)$, где n — мощность базы данных, являются случайными n-мерными векторами с независимыми координатами из интервала $(0,1)$ и задаются функциями плотности распределения запросов f и элементов g.

В работах [2,3] автором были подробно исследованы классы задач, для которых функция роста средней сложности поиска является ограниченной функцией, и когда функция роста имеет порядок логарифма от мощности базы данных. Получены условия на функции f и g, при которых сложность оптимального информационного графа в среднем по классу имеет порядок логарифма от мощности базы данных. Уточнены эти условия до получения асимптотики такой сложности. Также автором показано, что для любого отрезка вида $[b, b+2]$, где b — вещественное число большее единицы, можно построить классы задач, на которых сложность оптимального алгоритма в среднем не выходит за пределы отрезка при увеличении мощности базы данных.

В этой статье предлагается вниманию результат, полученный автором в работе [4]. Построены классы возможных асимптотик

функций роста средней сложности поиска, которые, с одной стороны, являются неограниченно возрастающими функциями, с другой стороны, имеют порядок меньше, чем логарифм от мощности базы данных.

Семейство S возможных асимптотик промежуточных функций роста состоит из функций вида $r(\log_2 \log_2(n))$, где возрастающая, положительная и дифференцируемая функция $r(x)$, определенная на интервале $(x_0, +\infty)$, $x_0 \geq 0$, сохраняет асимптотику и имеет в качестве производной монотонную, положительную и непрерывную функцию $r'(x)$, удовлетворяющую условию: для любого вещественного α, $\alpha > 0$, верхний предел отношения $r'(x)/(x^\alpha)$ меньше единицы при $x \to +\infty$.

Все функции из S являются неограниченно возрастающими и имеют порядок меньше, чем $\log_2 n$ при $n \to \infty$. Для каждой функции $s(n)$ из семейства S построен класс задач, асимптотика функции роста которого такая же, как у функции $s(n)$. Обозначим через $M_V T_n^{(f,g)}(V))$ математическое ожидание сложности поиска по классу задач $\Upsilon_n(f, g)$.

Теорема. *Для любой функции* $s(n) = r(\log_2 \log_2(n))$ *из семейства* S *существуют функции плотности* f *и* g, *такие что*

$$M_V T_n^{(f,g)}(V)) \sim r(\log_2 \log_2(n)) \quad (n \to \infty).$$

Также в качестве примера приводится подсемейство функций вида

$$c \cdot (\underbrace{\log_2 \ldots \log_2}_{i+1} n)^\alpha,$$

где α и c — вещественные положительные числа, а i — натуральное число.

Автор выражает благодарность своему научному руководителю профессору Гасанову Эльяру Эльдаровичу за постановку задачи и внимание к работе.

Список литературы

1. Гасанов Э. Э., Кудрявцев В. Б. Теория хранения и поиска информации. — М.: Физматлит, 2002.

2. Кучеренко Н. С. Сложность поиска идентичных объектов в случайных базах данных // Интеллектуальные системы. — 2007. — Т. 11, № 1–4. — С. 495–516.

3. Кучеренко Н. С. Средняя сложность поиска идентичных объектов для случайных неравномерных баз данных // Дискретная математика. — В печати.

4. Кучеренко Н. С. О промежуточных функциях роста сложности поиска для случайных баз данных // Интеллектуальные системы. — В печати.

О СВОЙСТВЕ УСТОЙЧИВОСТИ ДЛЯ СХЕМ ФУНКЦИОНАЛЬНЫХ ЭЛЕМЕНТОВ В k-ЗНАЧНОЙ ЛОГИКЕ

А. А. Лебедев (Москва)

Важным аспектом практического использования любой модели является ее устойчивость. Достаточно очевидно, что при практическом применении любой модели и идентификации ее параметров возникают (маленькие) ошибки измерения. Если модель чувствительна к такого рода естественным ошибкам, вопрос ее практического применения является проблематичным. В настоящей работе исследуется вопрос устойчивости дискретных иерархических систем, моделируемых схемами функциональных элементов (СФЭ).

Формальная постановка задачи в выбранной формализации имеет следующий вид:

Дана $F(x_1, ..., x_N)$ — функция k-значной логики, заданная схемой функциональных элементов над некоторым базисом B, состоящим из функций от не более, чем n переменных. Для заданного $1 \le A \le k-2$ необходимо проверить, удовлетворяет ли F следующему условию (назовём его A-устойчивостью):

$$\forall \alpha, \beta \in E_k^N \max_{i=1,...,N} |\alpha_i - \beta_i| \le A \Rightarrow |F(\alpha_1, ..., \alpha_N) - F(\beta_1, ..., \beta_N)| \le A$$

Класс всех A-устойчивых функций обозначим R_k^A, а класс всех A-устойчивых функций от n (фиксированных) переменных обозначим $R_k^A(n)$. Следующая теорема даёт оценку мощности рассматриваемых классов.

Теорема. $\frac{k-A}{A+1}(A+1)^{k^n} \le |R_k^A(n)| \le \frac{k-A}{2A+1}(A+1)^{k^n}(2A+1)^{\lceil \frac{k-1}{A} \rceil^n}$.

Следствие. $ln|R_k^A(n)| \sim k^n \sim \ln|P_k(n)|$.

Следующие две теоремы утверждают, что класс R_k^A является критериальным относительно разрешимости задачи проверки устойчивости эффективным алгоритмом.

Из замкнутости классов R_k^A непосредственно следует достаточное условие A-устойчивости функции, реализованной схемой.

Теорема. *Если все функции, вычисляемые элементами схемы, A-устойчивы, то реализуемая схемой функция также A-устойчива.*

Теорема. $\forall f(x_1, ..., x_m), m \leq n, f \in P_k \setminus R_k^A$ *задача проверки A-устойчивости для функций, заданных СФЭ над множеством* $f \cup R_k^A(2) \cup R_k^A(1)$, *co-NP-полна.*

Предыдущие результаты показывают, что внесение нетривиальных ограничений на базис СФЭ не приводит к существенному упрощению задачи проверки устойчивости. Следующая теорема показывает, что, внеся ограничения на графовую структуру СФЭ, задачу можно решать за линейное (от числа элементов схемы) время.

Теорема. *Для СФЭ, граф которых является деревом, существует алгоритм, решающий задачу проверки устойчивости, за время* $C(n) \cdot |V|$, *где* $|V|$ *— число вершин,* $C(n)$ *— величина, зависящая только от* n *— максимального числа переменных базисной функции.*

Теорема. *Для СФЭ, в графе которых циклы имеют длину не больше* l, *существует алгоритм, решающий задачу проверки устойчивости, за время* $C(n) \cdot |V| \cdot k^{n^l}$, *где* $|V|$ *— число вершин,* $C(n)$ *— величина, зависящая только от* n *— максимального числа переменных базисной функции.*

Теорема. *Для СФЭ k-значной логики, в графе которых имеется не более с циклов, существует алгоритм, решающий задачу проверки устойчивости, за время* $C(n) \cdot |V| \cdot k^c$, *где* $|V|$ *— число вершин,* $C(n)$ *— величина, зависящая только от* n *— максимального числа переменных базисной функции.*

Список литературы

1. Кудрявцев В. Б. Функциональные системы. — М.: Издательство Московского университета, 1982.

2. Лебедев А. А. О задачах оптимального распределения ресурсов и проверки устойчивости для схем функциональных элементов в k-значной логике // Интеллектуальные системы. — В печати.

3. Рыжов А. П. Об агрегировании информации в нечетких иерархических системах // Интеллектуальные системы. — 2002. — Т. 6, вып. 1–4. — С. 341–364.

4. Яблонский С. В. Основные понятия кибернетики // Проблемы кибернетики. Вып. 2. — 1959. — С. 7–38.

5. Ryjov A. Basic principles and foundations of information monitoring systems // Monitoring, Security, and Rescue Techniques in Multiagent Systems. — Springer, 2005. — P. 147–160.

О ВЫРАЗИМОСТИ СУПЕРПОЗИЦИЯМИ АВТОМАТОВ С ЦИКЛИЧЕСКИМИ ГРУППАМИ

А. А. Летуновский (Москва)

Рассматривается задача выразимости конечного автомата A суперпозициями системы $\Phi \cup \nu$, где Φ состоит из истинностных функций и "задержки", ν — произвольная конечная система автоматов. Ранее автор показал, что для автомата A с безусловными переходами существует алгоритм проверки $A \in [\Phi \cup \nu]$. В настоящей работе решается задача выразимости через систему $\Phi \cup \nu$ автомата A с циклической группой.

Пусть $E_k = \{0, 1, ..., k-1\}$, функции вида $g : E_k^n \to E_k$ называются функциями k- значной логики, их множество обозначается через P_k. Пусть E_k^∞ — множество всех сверхслов вида $a(1)a(2)...$, где $a(j) \in E_k$, $j = 1, 2, ...$ Через N обозначим множество натуральных чисел. Пусть $f : (E_k^\infty)^n \to (E_k^\infty)^m$ — автоматная функция (a-функция), т. е. она задается рекуррентно соотношениями (1):

$$\begin{cases} q_1(1) = q0_1, \\ ... \\ q_s(1) = q0_s \\ q_1(t+1) = \phi_1(q_1(t), ..., q_s(t), a_1, ..., a_n), \\ ... \\ q_s(t+1) = \phi_s(q_1(t), ..., q_s(t), a_1, ..., a_n) \\ b_1(t) = \psi_1(q_1(t), ..., q_s(t), a_1, ..., a_n) \\ ... \\ b_m(t) = \psi_m(q_1(t), ..., q_s(t), a_1, ..., a_n) \end{cases} \qquad (1)$$

Вектор $q = (q_1, ..., q_s)$ задает состояние a-функции f, $q0$ её начальное состояние, буквы $a = (a_1, a_2..., a_n)$ и $b = (b_1, ..., b_m)$ называют входной и выходной буквами, а сверхслова $a(1)a(2)...$ и $b(1)b(2)...$ — входными и выходными сверхсловами, соответственно. Вектор-функции ϕ и ψ называются функциями переходов и выходной функцией, соответственно, а шестерка $(E_k^n, E_k^s, E_k^m, \phi, \psi, q0)$ — автоматом, порождающим функцию f. Далее в тексте мы иногда будем использовать для автомата обозначение $(A, Q, B, \phi, \psi, q0)$, при этом предполагая что $A \subseteq E_k^n, Q \subseteq E_k^s, B \subseteq E_k^m$. Обычным образом доопределим функции ϕ и ψ на слова:
$\phi(q, a(1)...a(t)) = \phi(\phi...\phi(q, a(1)), ..., a(t-1)), a(t))$,
$\psi(q, a(1), ..., a(t)) = \psi(\phi(q, a(1)), ..., a(t-1)), a(t))$
и определим рекурсивно функцию
$\overline{\psi}(q, a(1), ..., a(t)) = \overline{\psi}(q, a(1), ..., a(t-1))\psi(\phi(q, a(1)...a(t-1)), a(t))$.
Класс всех a-функций обозначим через P.

В этом классе обычным образом введем операции суперпозиции:
$(\eta f)(x_1, x_2, .., x_n) = f(x_2, x_3, ..., x_n, x_1)$,
$(\varepsilon f)(x_1, x_2, .., x_n) = f(x_2, x_1, x_3, ..., x_n)$,
$(\varpi f)(x_1, x_2, .., x_n) = f(x_1, x_3, .., x_n)$,
$(\delta f)(x_1, x_2, .., x_n) = f(x_1, x_2, .., x_{n+1})$,
$(f * g)(x_1, x_2, .., x_{m+n-1}) = f(g(x_1, ..., x_m), x_{m+1}, ..., x_{m+n-1})$.

Пусть $M \subseteq P$, обозначим через $[M]$ множество a-функций, получающихся из M с помощью операций суперпозиции.

Автоматную функцию G_0, задаваемую уравнениями

$$\begin{cases} q(1) = 0, \\ q(t+1) = a(t), \\ b(t) = q(t), \end{cases}$$

назовём автоматной функцией задержки.

Константной автоматной функцией назовем автоматную функцию, выдающую одно и тоже периодическое выходное сверхслово на всех входных сверхсловах. Класс константных автоматных функций обозначим через K.

Через β_{K_1} обозначим сверхслово, получающееся на выходе константного автомата K_1.

Для множества константных автоматных функций $K' \subseteq K$ обозначим через $\Theta(K')$ — множество длин минимальных периодов сверхслов $\{\beta_{K_i} : K_i \in K'\}$.

Из [5] известно, что для $M \subseteq P$ в случае $[M] \supseteq \{P_k, G_0\}, |M| < \infty$ задача выразимости константных автоматных функций является алгоритмически разрешимой,более того $\exists b_M, q_M \in N$, такие что

$$\Theta([M \cup \{P_k, G_0\}] \cap K) = \{t : t | b_M q_M^i, i = 0, 1, ..\}.$$

Число q_M назовем *главным цикловым индексом* замкнутого класса M, b_M назовем *частным цикловым индексом* замкнутого класса M. Обозначим $< M >= [M \cup \{P_k, G_0\}]$.

В работе [5] показано, что цикловые индексы b_M и q_M вычисляются по системе автоматов M.

Автоматом A_p будем называть автомат вида $(\{a, b\}, \{1, ..., p\}, \{1, ..., p\}, \phi, \psi, 1)$ $\phi(i, a) = i, \phi(i, b) = i + 1 (\mathrm{mod}\ p)$ $\psi(i, a) = \psi(i, b) = i$.

Мы будем рассматривать задачу выразимости для автоматов A_p и при условии, что у нас в распоряжении есть штрих Шеффера и задержка.

Теорема 1. *Пусть M — конечное множество автоматных функций Медведева, тогда $A_p \in < M >$ тогда и только тогда, когда $p | q_M^i$ для некоторого i.*

Теорема 2. *Пусть M — конечное множество автоматных функций Медведева, тогда существует алгоритм, позволяющий проверить свойство $A_p \in < M >$.*

Автор выражает благодарность Кудрявцеву В. Б. и Бабину Д. Н. за ценные замечания и внимание к работе.

Список литературы

1. Кратко М. И. Алгоритмическая неразрешимость проблемы распознавания полноты для конечных автоматов // ДАН СССР. — 1964. — Т. 155, № 1. — С. 35–37.

2. Кудрявцев В. Б., Алешин С. В., Подколзин А. С. Введение в теорию автоматов. — М.: Наука, 1985.

3. Бабин Д. Н. О полноте двухместных автоматных функций относительно суперпозиции // Дискретная матетматика. — 1989. — Т. 1, вып. 4. — С. 423–431.

4. Летуновский А. А. О выразимости константных автоматов // Интеллектуальные системы. — 2005. — Т. 9, вып. 1–4. — С. 457–469.

5. Летуновский А. А. Разрешимый случай задачи выразимости автоматных функций относительно суперпозиции // Интеллектуальные системы. — В печати.

ПОВЫШЕНИЕ КРИПТОСТОЙКОСТИ ПРОТОКОЛА ЦИФРОВОЙ ПОДПИСИ НА ЭЛЛИПТИЧЕСКИХ КРИВЫХ

В. Ю. Лёвин (Москва)

В работе представлено решение проблемы по обеспечению подлинности цифровой информации с использованием эллиптических кривых. Большинство стандартных решений (DSA) основаны на сложности дискретного логарифмирования в мультипликативной группе конечного поля. Однако, современное развитие цифровой техники ставит под сомнение криптографическую надежность подобных систем. Для решения возникающей проблемы предлагается использовать вместо мультипликативной группы конечного поля группу точек эллиптической кривой заданной над конечным полем. В работе проведеннно подробное исследование изменения величины криптостойкости при подобном переходе. Обнаружено, что при переходе на эллиптические кривые, можно добиться серьезного увеличения криптостойкости подобных систем используя при этом

ключи меньшей длинны. Численно установлено, что для достижения заданного уровня криптостойкости (без перехода на эллиптические кривые), оставаясь в рамках мультипликативной группы конечного поля нужно существенно увеличивать размер используемых в криптосистеме ключей. Данная особенности является серьезным недостатком, ведь оперирование в полях большой размерности невозможно для маломощных микропроцессоров и большинства современных мобильных цифровых устройств. Для дальнейшего решения задачи обеспечения подлинности цифровой информации классическая схема цифровой подписи (DSA) переведена на эллиптические кривые. Подобная схема используется в уже имеющимся стандарте цифровой подписи на эллиптических кривых (ECDSA), однако она является малоизученной и имеет несколько существенных недостатков. Как известно, протокол цифровой подписи (DSA) является частным случаем классического протокола цифровой подписи Эль-Гамаля. Поэтому в работе изучается схема цифровой подписи Эль-Гамаля, которая вместе с множеством ее модификаций переведена на эллиптические кривые. В полученных модификациях обнаружено несколько существенных недостатков. Первый и очень существенный недостаток заключается в использующейся в схеме цифровой подписи однонаправленной хеш-функции. Известно, что большинство использующихся в криптографии хеш-функций имеет конечный порядок своего хеш-значения, поэтому использование подобных хеш-функций является слабым звеном всего протокола цифровой подписи. В работе приводится анализ большинства криптографических хеш-функций, например таких как (MD2, MD4, MD5 ,SHA1, SHA2, RIPEMD, HAVAL, TIGER, GOST). Для приведенных однонаправленных хеш-функций разработаны методики (метод последовательной префиксной суперпозиции, метод конкантенации, метод перестановок, метод суперпозиции перестановок и префиксных суперпозиций), позволяющие увеличить их криптостойкость в нужное число раз. Ключевой особенностью данных методов является то, что повышение криптостойкости хеш-функции (увеличение размера ее хеш-значения) добивается без изменения их внутренних алгоритмов, что позволяет реанимировать использование таких хеш-функций как (MD2, MD4, MD5, SHA1, HAVAL и т. д.). Данное свойство является ключевым, ведь перечисленные хеш-функции зашиты в железо, различные библиотеки и приложения, и изменение их алгоритмов не всегда является возможным. Второй, не менее существенный, недостаток заключается в заведомой слабости классической схемы цифровой подписи Эль-Гамаля и ее модификаций к фальсификации сообщений в процессе реализации протокола. Дей-

ствительно, злоумышленнику известно цифровое сообщение и его хеш-значение, ведь, согласно протоколу цифровой подписи, эти данные являются открытыми. После перехвата подобной информации, либо заготовки заранее, злоумышленник в состоянии обладать двумя текстами $M_1 \neq M_2, M_i \in \{0,1\}^*,\ i = 1,2$, причем по построению $h(M_1) = h(M_2)$, где $h(M) : \{0,1\}^* \to \{0,1\}^\delta$ — однонаправленная хеш-функция порядка δ. Далее злоумышленнику не составляет труда получив хеш-значение одного текста, подставить в протокол цифровой подписи Эль-Гамаля другой (нужный ему) текст с правильным хеш-значением. После чего, как в мультипликативной группе конечного поля, так и в группе точек эллиптической кривой над конечным полем, работа протокола цифровой подписи Эль-Гамаля не распознает подобной фальсификации. Предложен метод, позволяющий избавиться от указанного недостатка, без серьезного изменения логики стандартного протокола цифровой подписи Эль-Гамаля (логика процедуры генерации и верификации нового протокола цифровой подписи останется без серьезного изменения). В результате получена новая схема цифровой подписи Эль-Гамаля, устойчивая к фальсификации подписываемых сообщений как в процессе ее реализации, так и при сеансовой передаче. Криптостойкость полученной схемы алгоритма цифровой подписи на эллиптических кривых может быть подобрана под требования поставленной задачи, то есть является варьируемой величиной. Следует также отметить, что приведенные в настоящей статье механизмы улучшения алгоритма цифровой подписи Эль-Гамаля будут иметь место и в других алгебраических структурах, таких как мультипликативная группа конечного поля, группа точек эллиптической кривой, якобиан алгебраической кривой.

РЕШЕНИЕ АВТОМАТНЫХ УРАВНЕНИЙ

И. В. Лялин (Москва)

Пусть дана произвольная автоматная схема S, построенная из автоматов с помощью операций суперпозиции и обратной связи. Пусть в S выделено произвольное множество автоматов $x_1, x_2, \ldots, x_n$. Автоматы из этого множества будем называть *свободными позициями*, а остальные автоматы в схеме S — *фиксированными*. Схему S со свободными позициями будем обозначать так: $S(x_1, \ldots, x_n)$.

Пусть вместо автоматов x_i разрешается подставлять в схему S любые другие автоматы с тем же числом входов и выходов. То есть если у автомата x_1 имеется a_1 входов и b_1 выходов, то вместо него разрешается подставлять любой автомат c_1, у которого a_1 входов и b_1 выходов, при этом i-й вход автомата c_1 подключается в схему туда где раньше был подключен i-й вход автомата x_1, а j-й выход автомата u подключается в схему туда где раньше был подключен j-й выход автомата x_1. Пусть каждый x_i заменен таким образом на какой-то автомат c_i. Тогда если все обратные связи в схеме S окажутся корректными, то схема S станет эквивалентна некоторому автомату h. Будем это записывать так: $S(c_1, \ldots, c_n) = h$. Основная задача, рассматриваемая в данной работе, ставится следующим образом: дана схема со свободными позициями $S(x_1, \ldots, x_n)$ и автомат h, требуется найти все такие наборы автоматов $c_1, \ldots, c_n$, чтобы $S(c_1, \ldots, c_n) = h$. Таким образом, функционирование автоматов x_i нам не важно, они используются только как позиции, вместо которых подставляются автоматы c_i. Можно даже сказать что x_i — это переменные со значением в множестве всех автоматов, имеющих определенное число входов и выходов. А $S(x_1, \ldots, x_n) = h$, таким образом, есть уравнение с n неизвестными, которое требуется решить. Будем такие уравнения называть *автоматными*. Любой набор автоматов $c_1, \ldots, c_n$, такой, что $S(c_1, \ldots, c_n) = h$, называется *решением* автоматного уравнения $S(x_1, \ldots, x_n) = h$.

Основные полученные результаты.

Теорема 1. *Существует алгоритм построения полного описания всех решений любого автоматного уравнения с одной неизвестной.*

Теорема 2. *Не существует алгоритма, который для любого автоматного уравнения с двумя неизвестными устанавливает, имеется ли у данного уравнения хотя бы одно решение.*

Как следствие последней теоремы легко получить, что проблема существования решения у автоматных уравнений с более чем двумя неизвестными также алгоритмически неразрешима.

Автор выражает благодарность профессору Э. Э. Гасанову за помощь в работе.

Список литературы

1. Лялин И. В. О решении автоматных уравнений // Дискретная математика. — 2004. — Т. 16, вып. 2. — С. 104–116.

2. Лялин И. В. Решение автоматных уравнений с одной неизвестной // Интеллектуальные системы. — 2008. — Т. 12, вып. 1–4. — С. 271–282.

ОБ АДАПТИВНОЙ ЦИФРОВОЙ ОБРАБОТКЕ СИГНАЛОВ

И. Л. Мазуренко (Москва)

Адаптивная линейная система с обратной связью представляет собой адаптивный алгоритм, получающий на вход разность результата обработки входного сигнала x некоторым устройством обработки информации и требуемого выходного сигнала d ($x - d = \varepsilon$ — сигнал ошибки), и итерационно подстраивающий параметры устройства обработки информации с целью минимизации сигнала ошибки [1].

Примерами адаптивных систем являются системы линейного предсказания сигнала, широко применяющаеся при цифровом кодировании речи, системы моделирования и идентификации, применяющиеся для изучения вибраций механических системы, системы выравнивания характеристик, использующиеся для исключения влияния каналов связи, системы подавления шумов и помех, применяющиеся в задачах адаптивной шумоочистки и адаптивного эхоподавления. Рассмотрению алгоритмических подходов к решению последней задачи и посвящена настоящая работа.

В задаче адаптивной линейной фильтрации предполагается, что устройство обработки входной информации — линейно, и адаптивный алгоритм используется для итеративного подстраивания параметров этой линейной системы, а именно коэффициентов $H = (h_0, \dots h_{L-1})$ линейного фильтра с конечной импульсной характеристикой. При этом выходной сигнал y в момент времени k получается путем свертки входного сигнала x и коэффициентов фильтра: $y_k = \sum_{l=0}^{L-1} h_l x_{k-l}$. Наиболее распространенным применением адаптивной линейной фильтрации на практике является задача подавления эхо-сигнала в телефонных (проводных и беспроводных) сетях. Эхо в таких сетях делится на электрическое (возникающее в т. н. "гибридах" — устройствах преобразования 2-проводных телефонных сетей в 4-проводные) и акустическое (возникающее в оконечном оборудовании: мобильных и стационарных телефонах, устройствах обратной связи, оконечных устройствах IP-телефонии).

Адаптивные алгоритмы подстройки параметров линейного фильтра основываются на принципе минимизации квадрата сигнала ошибки ε. В качестве параметра сигнала ошибки рассматривают оценку величины среднеквадратического отклонения сигнала $E(\varepsilon_k^2) = E(d_k^2) + H^T E(X_k X_k^T) H - 2E(d_k X_k^T) H$.

Поскольку величина среднеквадратического отклонения сигнала ошибки представляет собой положительно определенную квадра-

тичную форму от коэффициентов фильтра H, минимум квадрата ошибки достигается в точке равенства нулю градиента $\nabla(\varepsilon_k^2) = 2RH - 2P$, где $R = E(X_k X_k^T)$ — $(L \times L)$-матрица автокорреляции, $P = E(d_k X_k^T)$ — корреляция эхо и требуемого выходного сигнала d. Это дает нам известную теорему Винера—Хопфа [1], позволяющую найти "идеальный" фильтр H, минимизирующий квадрат ошибки предсказания: $H = R^{-1}P$.

Поскольку на практике ни оценка матрицы автокорреляции R, ни вектор P точно неизвестны, используют итерационные методы, в той или иной степени сводящиеся к применению метода градиентного спуска: $H_{k+1} = H_k + \mu(-\nabla_k)$, $0 < \mu < \frac{1}{\lambda_{max}}$, где λ_{max} — максимальное по модулю собственное значение матрицы а втокорреляции R.

Наиболее простой и распространенной модификацией метода градиентного спуска является т. н. "метод наименьших квадратов", который применительно к данной задаче сводится к тому, что в качестве оценки математического ожидания квадрата ошибки $E(\varepsilon_k^2)$ берется величина ε_k^2. Формула адаптивного обновления оценки коэффициентов фильтра получается значительно более простой вычислительно: $H_{k+1} = H_k - \mu\hat{\nabla}_k = H_k + 2\mu\varepsilon_k X_k$, $0 < \mu < tr(R)$, ибо требует $2L+2$ умножений. Более быстро сходящийся алгоритм нормализованных наименьших квадратов использует $2L+2$ умножений и одно деление: $H_{k+1} = H_k + 2\mu\varepsilon_k \frac{X_k}{\|X_k\|^2}$, $0 < \mu < 1$.

В конце XX – начале XXI века было предложено несколько алгоритмов цифровой обработки сигналов, более эффективных с точки зрения соотношения скорости сходимости и вычислительной сложности. К их числу можно отнести метод аффинных проекций [2], метод быстрых аффинных проекций [3, 4] и приближенные методы быстрых аффинных проекций, основанные на Теплицевом приближении оценки автокорелляционной матрицы R ([5] и др.).

Метод аффинных проекций, обладающий наивысшей из известных методов скоростью сходимости, имеет сложность $2LN + K_{inv}N^2$ умножений, где K_{inv} — сложность обращения матрицы, а потому практически неприменим на практике. Его упрощение — метод быстрых аффинных проекций — обладает уже линейной сложностью относительно размера проекции N и числа коэффициентов фильтра L — $2L + 20N$ умножений, — однако, не лишен недостатков, один из которых (неустранимое накопление ошибок при целочесленной реализации) делает его практически неприменимым. Приближенные методы алгоритма быстрых аффинных проекций, описанные

[5], лишены данного недостатка и дают сложность в лучшем случае $2L + 8N - 3$ умножений, однако не обладают стабильностью в случае быстроменяющегося по своим спектральным характеристикам входного сигнала x.

Автором данной работы была предложена модификация приближенного метода быстрых аффинных проекций, основанного на применении Теплицевого приближения автокорреляционной матрицы R, в котором, в отличие от алгоритма [5], на каждом шаге итерации алгоритма Левинсона—Дурбина испольнуется новое приближение автокорреляционной матрицы, а для контроля за сходимостью алгоритма применяется пороговое правило контроля уровня недекоррелированной ошибки адаптации. Данная модификация алгоритма, практически не проигрывая в скорости методу [5], дает на тестовых данных значительно более высокую скорость сходимости и надежность работы алгоритма адаптации. Работа защищена патентом США.

Список литературы

1. Уидроу Б., Стирнз С. Адаптивная обработка сигналов. — М.: Радио и связь, 1989.

2. Ozeki K., Umeda T. An adaptive filtering algorithm using an orthogonal projection to an affine subspace and its properties // Proc. of the Elec. Comm. Japan. — 1984. — V. J67-A. — P. 126–132.

3. Gay S. L. A fast converging, low complexity adaptive filtering algorithm // Third International Workshop on Acoustic Echo Control. — Plestin les Greves (France), 7–8 Sept. 1993.

4. Tanaka M., KanedaY., Makino S., Kojima J. A fast projection algorithm for adaptive filtering // IEICE Trans. Fund. — October 1995. — E78-A (10m).

5. Ding H. Fast affine projection adaptation algorithms featuring stable symmetric positive-definite linear system solvers // Applications of Signal Processing to Audio and Acoustics. — 2005.

О ЧАСТИЧНОМ УГАДЫВАНИИ РЕГУЛЯРНЫХ ВЫРАЖЕНИЙ

А. А. Мастихина (Москва)

Рассматривается конечный автомат, на вход которого поступает бесконечная последовательность из нулей и единиц. Цель автомата

в каждый момент работы — предсказать следующий символ последовательности.

Выходное сверхслово автомата $\mathfrak{A}$ при подаче на его вход сверхслова α будем обозначать через $y_\alpha^{\mathfrak{A}}$.

Автомат $\mathfrak{A}$ *угадывает сверхслово* $\alpha \in \{0,1\}^\infty$, если

$$\sum_{i=1}^{\infty} |y_\alpha^{\mathfrak{A}}(i) - \alpha(i+1)| < \infty.$$

В [1] было доказано, что угадывающий автомат можно построить только для периодических сверхслов.

Автомат $\mathfrak{A}$ *угадывает сверхслово* $\alpha \in \{0,1\}^\infty$ *со степенью* $\sigma \in [0,1]$, если

$$c^{\mathfrak{A}}(\alpha) = \underline{\lim}_{t\to\infty} \frac{1}{t} \sum_{i=1}^{t} (1 - |y_\alpha^{\mathfrak{A}}(i) - \alpha(i+1)|) = \sigma.$$

Автомат частично угадывает множество сверхслов, если степень угадывания каждого сверхслова из множества строго больше нуля. Множество сверхслов частично угадываемо, если существует автомат, частично угадывающий это множество.

Рассмотрим общерегулярное выражение вида $(a_1 \cup a_2 \cup \ldots \cup a_s)^\infty$, где $s \in \mathbb{N}$, $a_i \in \{0,1\}^*$, $i = \overline{1,s}$.

За s_t обозначим количество слов длины t, за l — максимальную длину слов a_i. В случае, если ни одно a_i не является префиксом никакого другого, степень можно оценить следующим образом.

Теорема 1. *Дано общерегулярное выражение вида* $A = (a_1 \cup a_2 \cup \ldots \cup a_s)^\infty$, *где ни одно* a_i *не является префиксом никакого* a_j *Множество сверхслов, образованное* A, *частично угадываемо, если оно не задается выражением* $(0 \cup 1)^\infty$, *причем для любого сверхлова* $\alpha \in A$ *выполнено*

$$c^{\mathfrak{A}}(\alpha) \geqslant \min_{t=1..l, s_t \neq 0} \{\frac{t - [\log_2(\sum_{i=1}^{t} (2^{t-i} \cdot s_i)]}{t}\}.$$

В частном случае, когда $a_1, ..a_s$ — слова одинаковой длины l, множество сверхслов частично угадываемо со степенью $\sigma \geqslant \frac{l - \log_2 s}{l}$.

Теорема 2. *Пусть для некоторого конечного автомата* $\mathfrak{A}$ *и множества сверхслов, заданного выражением* $A = (a_1 \cup \ldots \cup a_s)^\infty$ *выполнено* $\min_{\alpha\in A} c^{\mathfrak{A}}(\alpha) = \sigma_1$, $\max_{\alpha\in A} c^{\mathfrak{A}}(\alpha) = \sigma_2$. *Тогда для каждого* $\sigma_0 \in [\sigma_1, \sigma_2]$ *найдется такое сверхслово* $\lambda \in A$, *что* $c^{\mathfrak{A}(\lambda)} = \sigma_0$.

Теорема 3. *Пусть дано множество* $A = (a_1 \cup ... \cup a_s)^\infty$. *Каждый конечный автомат* $\mathfrak{A}_i$ *угадывает это множество со степенью не меньшей чем* σ_i, *и пусть существует* $\sigma_0 = \max\limits_i \sigma_i$. *Тогда в данном множестве найдется такое сверхслово* λ, *что любой автомат угадывает его со степенью* $\leqslant \sigma_0$.

Автор выражает благодарность профессору Э. Э. Гасанову за постановку задачи и помощь в работе.

Список литературы.

1. Вереникин А. Г., Гасанов Э. Э. Об автоматной детерминизации множеств сверхслов // Дискретная математика. — 2006. — Т. 18, № 2. — С. 84–97.

2. Мастихина А. А. О частичном угадывании сверхслов // Интеллектуальные системы. — 2007. —Т. 11, вып. 1–4. — С. 609–619.

3. Кудрявцев В. Б., Алешин С. В., Подколзин А. С. Введение в теорию автоматов. — М.: Наука, 1985.

МЕТОД АНАЛИЗА СВОЙСТВ ФУНКЦИОНАЛЬНЫХ ПРОГРАММ

А. М. Миронов (Москва)

В докладе рассматривается новый подход к математическому моделированию функциональных программ (ФП) при помощи графовых моделей, и показывается, как можно использовать предложенный подход для решения задачи верификации ФП. Под задачей верификации ФП в настоящем докладе понимается задача построения формального доказательства утверждения о том, что две функции, определяемые различными ФП, совпадают. Данная задача рассматривалась в некоторых работах, среди которых отметим, например, [1–3]. Основным методом доказательства свойств ФП в данных работах являлся метод математической индукции. В настоящем докладе мы предлагаем другой метод доказательства свойств ФП, который можно рассматривать как обобщение известного метода Флойда для верификации императивных программ.

Под ФП в настоящем докладе мы понимаем систему уравнений

$$\begin{cases} f_1(x_{11}, \ldots, x_{1k_1}) = e_1, \\ \ldots \\ f_n(x_{n1}, \ldots, x_{nk_n}) = e_n, \end{cases} \tag{1}$$

которая представляет собой определение некоторого множества функций, где f_1, ..., f_n — функциональные символы, являющиеся именами определяемых функций, x_{11}, ..., x_{nk_n} — различные переменные, являющиеся формальными параметрами определяемых функций, и e_1, ..., e_n — выражения.

Графовой моделью (ГМ) ФП (1) называется граф, в котором каждая вершина имеет метку, совпадающую с некоторым подвыражением одного из выражений, входящих в (1), и каждое ребро имеет метку одного из следующих типов: 1) *условие*: метка данного типа имеет вид $\varphi\,?$ или $\neg\varphi\,?$, где φ либо некоторое подвыражение одного из выражений $e_1, \ldots, e_n$, либо константа 1; 2) *подстановка*: метка данного типа имеет вид

$$[x_1 := u_1, \ldots, x_m := u_m]$$

где x_1, ..., x_m — некоторые различные переменные, входящие в (1), и u_1, ..., u_m — некоторые подвыражения выражений, входящих в (1); 3) *ссылка на подвыражение*: метка данного типа имеет вид (i), и имеет следующий смысл: для каждого ребра с меткой (i) метка вершины, являющейся началом данного ребра, имеет вид $f(u_1, \ldots, u_m)$, и метка вершины, являющейся концом данного ребра, равна u_i.

ГМ строится по ФП (1) следующим образом.

1) Множество её вершин находится во взаимно-однозначном соответствии с множеством всех подвыражений выражений, входящих в (1). Меткой каждой вершины является соответствующее ей подвыражение.

2) Для каждого уравнения $f_i(x_{i1}, \ldots, x_{ik_i}) = e_i$, входящего в (1), ГМ содержит ребро с меткой 1? из вершины с меткой $f_i(x_{i1}$, ..., $x_{ik_i})$ в вершину с меткой e_i.

3) Для каждой вершины N с меткой вида `if` e_1 `then` e_2 `else` e_3 ГМ содержит ребро из N в вершину с меткой e_2, метка этого ребра равна $e_1?$, и ребро из N в вершину с меткой e_3, метка этого ребра равна $\neg e_1?$.

4) Для каждой вершины N с меткой вида $f_i(u_1, \ldots, u_{k_i})$, где f_i – имя одной из функций, определяемых в ФП (1), ГМ содержит ребро из N в вершину с меткой $f_i(x_{i1}$, ..., $x_{ik_i})$, метка этого ребра имеет вид $[x_{i1} := u_1, \quad \ldots, \quad x_{ik_i} := u_{k_i}]$.

5) Для каждой вершины N с меткой вида $f(u_1, \ldots, u_m)$, где f — имя одной из базовых функций, и каждого $i = 1, \ldots, m$ ГМ содержит ребро из N в вершину с меткой u_i, метка этого ребра равна (i).

Теорема, на которой основан метод верификации ФП, представляет собой набор условий, которым должны удовлетворять ГМ

двух ФП, в случае выполнения которых функции, определяемые этими ФП, совпадают.

Список литературы

1. Филд А., Харрисон П. Функциональное программирование. — М.: Мир, 1993.

2. van den Berg K. G., van den Broek P. M. Static analysis of functional programs // Information and Software Technology. — 1995. — V. 37, № 4. — P. 213–224.

3. Ireland A., Bundy A. Automatic verification of functions with accumulating parameters // Journal of Functional Programming. — 1999. — 9 (2). — P. 225–245.

К ВОПРОСУ ОБ АЛГОРИТМИЧЕСКОЙ РАЗРЕШИМОСТИ ПРОБЛЕМЫ ВЫРАЗИМОСТИ ДЛЯ ФУНКЦИЙ С ЗАДЕРЖКОЙ

С. В. Моисеев (Москва)

Обозначим через $P_k(m)$, где k — натуральное число, множество всех m-местных функций k-значной логики, пусть также P_k — множество всех функций k-значной логики. Пусть $\omega = \{0, 1, 2, \ldots\}$. Функция k-значной логики с задержкой — это пара $\langle f, t\rangle$, где $f \in P_k$, $t \in \omega$.

Рассмотрим на множестве P_k операции перестановки, отождествления и добавления фиктивных переменных [1]:

$$
\begin{aligned}
(\zeta f)\,\langle x_1, \ldots, x_m\rangle &\leftrightharpoons f\langle x_2, \ldots, x_m, x_1\rangle;\\
(\tau f)\,\langle x_1, \ldots, x_m\rangle &\leftrightharpoons f\langle x_2, x_1, x_3, \ldots, x_m\rangle;\\
(\Delta f)\,\langle x_1, \ldots, x_{m-1}\rangle &\leftrightharpoons f\langle x_1, x_1, \ldots, x_{m-1}\rangle;\\
(\nabla f)\,\langle x_1, \ldots, x_{m+1}\rangle &\leftrightharpoons f\langle x_2, \ldots, x_{m+1}\rangle.
\end{aligned}
$$

Распространим эти операции на функции с задержкой: $\zeta\langle f, t\rangle \leftrightharpoons \langle \zeta f, t\rangle$, $\tau\langle f, t\rangle \leftrightharpoons \langle \tau f, t\rangle$, $\Delta\langle f, t\rangle \leftrightharpoons \langle \Delta f, t\rangle$, $\nabla\langle f, t\rangle \leftrightharpoons \langle \nabla f, t\rangle$ и введём частичную операцию *синхронной суперпозиции* $*$: скажем, что операция $*$ применима к $\langle f^{(n)}, t\rangle$ и набору $\langle\langle g_1^{(m)}, t_1\rangle, \ldots, \langle g_n^{(m)}, t_n\rangle\rangle$, если $t_1 = t_2 = \ldots = t_n$, и в случае применимости положим

$$
\langle f^{(n)}, t\rangle * \langle\langle g_1^{(m)}, t_1\rangle, \ldots, \langle g_n^{(m)}, t_n\rangle\rangle \leftrightharpoons \langle f * \langle g_1, \ldots, g_n\rangle,\ t + t_1\rangle,
$$

где $f * \langle g_1, \ldots, g_n \rangle$ — результат подстановки функций $g_1, \ldots, g_n$ в функцию f, а именно: $(f * \langle g_1, \ldots, g_n \rangle)\alpha \leftrightharpoons f\langle g_1\,\alpha, \ldots, g_n\,\alpha \rangle$.

На множестве $P_k \times \omega$ стандартным образом вводим оператор $[]_{cc}$ замыкания относительно операций $\zeta, \tau, \Delta, \nabla, *$: для каждого $M \subseteq P_k \times \omega$ множество $[M]_{cc}$ определяется как наименьшее множество, содержащее M и замкнутое относительно указанных операций.

Основной исследуемой задачей является задача *выразимости*: дано множество $M \subseteq P_k \times \omega$ и $\langle f, t \rangle \in P_k \times \omega$; спрашивается, верно ли, что $\langle f, t \rangle \in [M]_{cc}$. В настоящей работе показано, что данная задача для конечных множеств M алгоритмически разрешима.

Впервые проблема выразимости для функций с задержкой исследовалась Кудрявцевым В. Б. (см., например, монографию [2]). Традиционно при исследовании алгоритмической разрешимости проблемы полноты для функций многозначных логик и функций с задержками используется аппарат предполных классов и сохранения отношений. В данной же работе предлагается иной подход к доказательству алгоритмической разрешимости этих задач — построение строгого логического языка для функций с задержками, достаточно выразительного, для того чтобы на нём можно было сформулировать проблему выразимости, для которого впоследствии доказывается наличие алгоритма, проверяющего истинность формул этого языка.

Формальный язык для функций с задержкой. Для натурального числа m рассмотрим сигнатуру $\langle \mathfrak{F}^{(1)}, \mathfrak{Z}^{(2)}, \sim^{(2)}, \mathfrak{u}_1, \ldots, \mathfrak{u}_m \rangle$, содержащую два функциональных символа $\mathfrak{F}$, $\mathfrak{Z}$, предикатный символ $\sim$ и m константных символов $\mathfrak{u}_1, \ldots, \mathfrak{u}_m$; и пусть $\Phi\mathfrak{Z}(m)$ — монадический второпорядковый язык этой сигнатуры (то есть язык логики предикатов, в котором разрешено использование кванторов по предметным переменным, которые мы обозначаем строчными буквами, и по одноместным предикатам, обозначаемым прописными буквами).

Определим для языка $\Phi\mathfrak{Z}(m)$ интерпретацию: носителем выступает множество $P_k(m) \times \omega$, а функциональные, предикатный и константные символы $\mathfrak{F}$, $\mathfrak{Z}$, $\sim$, $\mathfrak{u}_1, \ldots, \mathfrak{u}_m$ интерпретируются соответственно функциями $\underline{\mathfrak{F}}$, $\underline{\mathfrak{Z}}$, предикатом $\simeq$ и функциями $\underline{\mathfrak{u}_1}, \ldots, \underline{\mathfrak{u}_m}$, где

$$\underline{\mathfrak{F}}\,\langle\langle f_1, t_1\rangle, \langle f_2, t_2\rangle\rangle \leftrightharpoons \begin{cases} \langle F_u\langle f_1, f_2\rangle, t_1\rangle, & t_1 = t_2; \\ \langle f_1, t_1\rangle, & t_1 \neq t_2. \end{cases}$$

$$\underline{\mathfrak{Z}}\,\langle f, t\rangle \leftrightharpoons \langle f, t+1\rangle,$$

$$\langle f_1, t_1\rangle \simeq \langle f_2, t_2\rangle \leftrightharpoons t_1 = t_2,$$

$$\underline{\mathfrak{u}_i}\,\langle \alpha^1, \ldots, \alpha^m\rangle \leftrightharpoons \alpha^i \quad (i \in \{1, \ldots, m\}),$$

где $F_u\colon P_k \times P_k \to P_k$ — оператор подстановки в универсальную функцию: $F_u\langle f_1, f_2\rangle\,\alpha \leftrightharpoons U_k\langle f_1\,\alpha, f_2\,\alpha\rangle$, а U_k — некоторая, изначально выбранная для данного k, универсальная функция k-значной логики (функция, образующая полную систему относительно суперпозиции). Будем обозначать эту интерпретацию через $P_k(m) \times \omega$.

Выразительные свойства языка ФЗ(m). Пусть $M = \{\tau_1, \ldots, \tau_n\}$ — конечное множество термов над $\{\mathfrak{Z}^{(1)}, \mathfrak{F}^{(2)}, \mathfrak{u}_1, \ldots, \mathfrak{u}_m\}$. Рассмотрим формулы

$$\text{Замк}_M(X) =$$
$$\forall f_1 \ldots \forall f_m \Big(\Big(\bigwedge_{k=1}^{m} X\, f_k \wedge \bigwedge_{k=1}^{r-1} f_k \sim f_{k+1}\Big) \to \bigwedge_{k=1}^{n} X\, \tau_k(f_1, \ldots, f_m)\Big),$$

где $\tau_k(f_1, \ldots, f_m)$ — результат замены в терме τ_k всех вхождений символов $\mathfrak{u}_1, \ldots, \mathfrak{u}_m$ на $f_1, \ldots, f_m$ соответственно.

$$(X = [M]_{cc}) \leftrightharpoons \bigwedge_{\tau \in M^*} X\,\tau \wedge \text{Замк}_M(X) \wedge$$
$$\wedge\, \forall Y \Big(\Big(\bigwedge_{\tau \in M^*} Y\,\tau \wedge \text{Замк}_M(Y)\Big) \to \forall f\big(X\, f \to Y\, f\big)\Big),$$

где $M^* \leftrightharpoons \{\tau(a_1, \ldots, a_m) \mid \tau \in M;\ a_1, \ldots, a_m \in \{\mathfrak{u}_1, \ldots, \mathfrak{u}_m\}\}$ (конечное множество).

Разрешимость теории функций с задержкой. Основной результат настоящего исследования состоит в том, что существует алгоритм, проверяющий по формуле языка ФЗ(m), истинна ли она в интерпретации $P_k(m)$ или нет, более того справедливо

Утверждение 1. *Существует вычислимый предикат A, такой что для всех натуральных k и m и монадической второпорядковой формулы φ сигнатуры $\langle \mathfrak{F}^{(1)}, \mathfrak{Z}^{(2)}, \sim^{(2)}, \mathfrak{u}_1, \ldots, \mathfrak{u}_m\rangle$*

$$A\langle k, m, \varphi\rangle \leftrightarrow \big(P_k(m) \times \omega \models \varphi\big).$$

А поскольку в языке ФЗ(m) можно эффективно сформулировать свойство выразимости: $\big(\tau \in [M]_{cc}\big) \leftrightharpoons \exists X\big(\big(X = [M]_{cc}\big) \wedge X\,\tau\big)$, из существования алгоритма, проверяющего истинность этой формулы автоматически вытекает

Утверждение 2. *Проблемы выразимости для функций с задержкой алгоритмически разрешима.*

Список литературы

1. Мальцев А. И. Итеративные алгебры и многообразия Поста // Алгебра и логика. — 1966. — Т. 5, № 2. — С. 5–24.

2. Кудрявцев В. Б. Функциональные системы. — М.: Издательство Московского университета, 1982.

О КОДИРОВАНИИ ДИСКРЕТНЫХ ФИГУР ОТРЕЗКАМИ

А. А. Муравьева (Москва)

На практике реальные геометрические образы аппроксимируются конечным множеством точек, и "похожесть" этих образов можно изучать на основе этих аппроксимаций. В качестве характеристики таких дискретных аппроксимаций возьмем множество попарных расстояний между точками. Отличие такой характеризации фигур от подробной, но более емкой характеризации с помощью симплексов состоит в том, что здесь в качестве кодов фигур выступают их одномерные характеристики. В случае характеристики симплексами и производными от них, возникает кодировка, восстанавливающая фигуры с точностью до аффинной эквивалентности [1].

Назовем множество A из n точек ($|A| = n$) n-образом. Выпишем все попарные расстояния между точками A в порядке убывания. Получим упорядоченный набор $S(A) = \{d_1, \ldots, d_N : d_1 \geq d_2 \geq \cdots \geq d_N\}$, который назовем спектром A. Графиком назовем произвольную невозрастающую конечную последовательность Γ положительных действительных чисел. A — модель для Γ, если спектр A совпадает с Γ (S(A)=Γ).

Теорема 1. *Существует алгоритм построения по графику всех его моделей в пространстве заданной размерности.*

Рассмотрим два способа продолжения графика до спектра путем добавления в него новых элементов. При первом способе элементы приписываются к началу графика, а при втором разрешено добавлять элементы "внутрь" графика. Введем величину J_Γ, равную минимальному числу элементов, которые необходимо приписать к Γ для продолжения его до спектра. Аналогично введем величину N_Γ, равную минимальному числу элементов, которые необходимо добавить в Γ для продолжения его до спектра. Положим

$$J(m) = \max_{|\Gamma|=m} J_\Gamma, \qquad N(m) = \max_{|\Gamma|=m} N_\Gamma.$$

Для этих величин найдены точные значения.

Теорема 2. $J(m) = C^2_{2(m-1)} - m$.

Теорема 3. $N(m) = C^2_{m+1} - m$.

Далее рассмотрим некоторые свойства графиков, являющихся спектрами.

Пусть $|\Gamma| = m$. Введем величину

$$const(\Gamma) = \max_{i=1,\dots,m} (j \in \mathbb{N} | d_i = \dots = d_{i+j-1}, 1 \le j \le m-i+1),$$

то есть длину максимального участка постоянства графика Γ.

Теорема 4. *Пусть $A \subseteq \mathbb{R}^2$. Тогда имеет место:*

1) $\forall A \ (const(\Gamma(A)) < 3|A|)$;

2) $\forall \varepsilon > 0 \ \exists N_\varepsilon \ \forall n \ge N_\varepsilon \ \exists A \ (|A| = n \quad и \quad const(\Gamma(A)) > (3-\varepsilon)n)$.

Пусть $const(n) = \max\limits_{A \subseteq \mathbb{R}^2 : |A| = n} const(A)$.

Следствие 1. $const(n) \sim 3n \quad$ при $n \to \infty$.

Следствие 2. *Если в графике $\Gamma = (d_1, d_2, \dots, d_{C^2_n})$ $const(\Gamma) > 3n$, то Γ не является спектром на плоскости.*

В качестве следующей характеристики графиков рассмотрим отношение максимального элемента графика к минимальному. Оказывается, что в графиках, являющихся спектрами, на значение этого отношения накладываются некоторые ограничения. Положим

$$R_m(n) = \inf_{A \subseteq \mathbb{R}^m : |A| = n} \frac{d_1(A)}{d_{C^2_n}(A)}, \text{ где } S(A) = (d_1(A), \dots, d_{C^2_{|A|}}(A)).$$

Оценки для этой величины в случае плоскости и трехмерного пространства содержатся в следующих теоремах.

Теорема 5. $R_2(n) > \sqrt{\frac{2\sqrt{3}}{\pi}}\sqrt{n} - \frac{4}{3}$.

Следствие. *Если для графика $\Gamma = (d_1, d_2, \dots, d_{C^2_n})$ выполняется условие $\frac{d_1}{d_{C^2_n}} < \sqrt{\frac{2\sqrt{3}}{\pi}}\sqrt{n} - \frac{4}{3}$, то Γ не является спектром на плоскости.*

Замечание. *Существует возрастающая подпоследовательность $\{n_k, \ k = 1, 2, \dots\}$ натуральных чисел, для которой*

$$R_2(n_k) \sim \sqrt{\frac{2\sqrt{3}}{\pi}}\sqrt{n_k} \quad при \ k \to \infty.$$

Теорема 6. $R_3(n) > \frac{4}{5}\sqrt[3]{n} - \frac{4}{5}$.

Следствие. *Если в графике* $\Gamma = (d_1, d_2, \ldots, d_{C_n^2})$ *выполнено условие* $\frac{d_1}{d_{C_n^2}} < \frac{4}{5}\sqrt[3]{n} - \frac{4}{5}$, *то* Γ *не является спектром в пространстве.*

Замечание. $R_3(n) \asymp \sqrt[3]{n}$ *при* $n \to \infty$.

Автор выражает благодарность своему научному руководителю Кудрявцеву В. Б. за постановку задачи, внимание к работе и ценные обсуждения.

Список литературы

1. Козлов В. Н. Математическое моделирование зрительного восприятия // Математические вопросы кибернетики. — 1996. — Вып. 6. — С. 321–338.

2. Муравьева А. А. Распознавание n-точечников // Интеллектуальные системы. — 2007. — Т. 11, вып. 1–4. — С. 777–780.

О РАСШИФРОВКЕ ОДНОГО КЛАССА ДИСКРЕТНЫХ ФУНКЦИЙ

В. В. Осокин (Москва)

Неформально *расшифровка функций из некоторого класса* Φ — это игра между учителем и учеником (алгоритмом расшифровки) [1]. Учитель загадывает некоторую функцию из класса Φ. Ученик должен полностью восстановить таблицу значений загаданной функции, задав учителю минимальное число вопросов (*запросов на значение функции*). Под запросом понимается точка из области определения функции, а *ответом* учителя является значение функции в данной точке.

Под *алгоритмом расшифровки* будем понимать условный эксперимент, который последовательно генерирует запросы на значение функции в зависимости от ответов на предыдущие запросы. Будем говорить, что алгоритм *расшифровывает* функцию f, если значения функции f на наборах из результата условного эксперимента (т.е., на множестве сгенерированных им запросов на значение функции) однозначно определяют таблицу значений функции f. Алгоритм расшифровки будем называть *безусловным*, если он является безусловным экспериментом. В противном случае будем называть его *условным*.

Определим класс Ψ^n дискретных функций, сопоставляющих каждой вершине куба $\{0,1\}^n$ натуральное число. Дискретная функция $f : \{0,1\}^n \to \mathbb{N}$ называется *граневой*, если для любых наборов $\alpha > \beta \in \{0,1\}^n$ и для любого набора $\gamma \in \{0,1\}^n$, такого что $\alpha > \gamma > \beta$, из $f(\alpha) = f(\beta)$ следует, что $f(\alpha) = f(\gamma)$. Другими словами, если функция принимает одно и то же значение на двух сравнимых наборах куба, то она принимает то же значение и на всей грани, образованной этими двумя наборами. Очевидно, что булевские монотонные функции, псевдо-булевские монотонные функции [2], а также разбивающие функции [3] являются граневыми. Класс всех граневых функций обозначим через Ψ.

В работе исследуется сложность расшифровки функций из Ψ^n при помощи запросов на значение функции.

Пусть $\varphi(F, f)$ — число запросов на значение функции, которое требуется алгоритму F для расшифровки функции $f \in \Psi$, $\mathcal{A}(\Psi)$ — множество алгоритмов, расшифровывающих все функции из Ψ. Положим $\varphi(\Psi, n) = \min\limits_{F \in \mathcal{A}(\Psi^n)} \max\limits_{f \in \Psi^n} \varphi(F, f)$. Заметим, что здесь использован min, а не inf, поскольку при фиксированном n число алгоритмов расшифровки функций из Ψ^n конечно. Функцию $\varphi(\Psi, n)$ будем называть *сложностью расшифровки* Ψ.

Утверждение. *Для любого* $n \in \mathbb{N}$ *выполнено* $\varphi(\Psi, n) = 2^n$.

Для практики особый интерес представляют функции из класса Ψ^n, число существенных переменных которых мало по сравнению с n. Поэтому, естественен вопрос о существовании параметро-эффективного [4] алгоритма расшифровки функций из Ψ^n, т.е. алгоритма, сложность которого слабо (например, логарифмически) зависит от числа несущественных переменных неизвестной функции. Пусть $\Psi^{k,n}$ — подмножество Ψ^n, состоящее из функций, зависящих существенно от не более чем k переменных. Положим $\varphi(\Psi, n, k) = \min\limits_{F \in \mathcal{A}(\Psi^n)} \max\limits_{f \in \Psi^{k,n}} \varphi(F, f)$. Мы показываем, что сложность расшифровки функций из $\Psi^{k,n}$ асимптотически не меньше $k \log n + 2^k$ и строим оптимальный по порядку параметро-эффективный алгоритм расшифровки функций из Ψ^n.

Теорема. *Для* $k, n \in \mathbb{N}$ *выполнено* $\varphi(\Psi, n, k) \asymp k \log n + 2^k$ *при* $n \to \infty$.

Интерес также представляет ситуация, в которой учитель может отвечать сразу на целый блок сгенерированных учеником запросов на значение функции. В такой ситуации встает вопрос минимизации числа блоков запросов на значение функции, подаваемых учеником учителю в процессе расшифровки (минимизации *парал-*

лельной сложности алгоритма расшифровки). Упомянутый выше оптимальный по порядку параметро-эффективный алгоритм расшифровки функций из Ψ^n является по существу условным: при выборе следующего запроса на значение функции он пользуется знаниями о значениях функции на предыдущих поданных им наборах. Отсюда следует, что его параллельная сложность не оптимальна. В идеале хотелось бы иметь безусловный параметро-эффективный алгоритм расшифровки, поскольку параллельная сложность такого алгоритма равна единице. Мы показываем, что безусловного близкого к оптимальному параметро-эффективного алгоритма расшифровки граневых функций не существует, доказываем зависимость сложности расшифровки от параллельной сложности и строим оптимальный по порядку параметро-эффективный алгоритм расшифровки граневых функций с оптимальной параллельной сложностью расшифровки.

Множество последовательно сделанных алгоритмом F запросов на значение функции при расшифровке функции f будем называть (F, f)-*независимым*, если при формировании каждого запроса из этого множества алгоритм расшифровки не использует информацию о значениях функции f на ранее поданных наборах из этого множества. Через $\varphi_p(F, f)$ обозначим минимальное число (F, f)-независимых множеств, таких что в объединении они дают все множество запросов, сделанных F при расшифровке f.

Обозначим $\mathcal{A}_q(\Psi, n, k) = \{F \in \mathcal{A}(\Psi^n) : \max\limits_{f \in \Psi^{k,n}} \varphi(F, f) \leq q\}$.

Положим $\varphi_p(\Psi, n, k, q) = \min\limits_{F \in \mathcal{A}_q(\Psi,n,k)} \max\limits_{f \in \Psi^{k,n}} \varphi_p(F, f)$.

Теорема. *Для $k, n \in \mathbb{N}$ и произвольной константы $c > 2$, такой что $2^k < (\frac{c}{2} - 1)k \log n$, выполнено $\varphi_p(\Psi, n, k, c \cdot k \log n) \asymp k$ при $k, n \to \infty$.*

Автор выражает благодарность профессору Э. Э. Гасанову за постановку задачи и помощь в работе.

Список литературы

1. Кудрявцев В. Б., Гасанов Э. Э., Подколзин А. С. Введение в теорию интеллектуальных систем. — М.: Изд-во ф-та ВМиК МГУ, 2006.

2. Foldes S., Hammer P. L. Monotone, horn and quadratic pseudo-Boolean functions // J. UCS. — 2000. — 6 (1). — P. 97–104.

3. Осокин В. В. Асимптотически оптимальный алгоритм расшифровки разбиения булевого куба на подкубы // Интеллектуальные системы. — 2007. —Т. 11. — С. 587–606.

4. Damaschke P. Adaptive versus nonadaptive attribute-efficient learning // Machine Learning. —2000. — 41. — P. 197–215.

ОБ ОБЪЕМНОЙ СЛОЖНОСТИ РЕАЛИЗАЦИИ МОНОТОННЫХ ФУНКЦИЙ

А. А. Охлопков (Москва)

В последнее время, все острее становятся вопросы улучшения и оптимизации процессоров ЭВМ. При этом важнейшей задачей является задача оптимизации сложности и объемов процессоров при сохранении ими высоких параметров обработки информации. Поскольку любой процессор представляет собой реализацию булевых функции, именно исследования реализации таких функций в виде схем из функциональных элементов представляются важной составляющей.

Из работ К. Э. Шеннона и О. Б. Лупанова известно, что большинство булевых функций допускает лишь очень сложную схемную реализацию. Поэтому разными авторами [1–3] вводились и изучались классы булевых функций существенно более узкие, чем множество всех булевых функций. Одним из таких известных классов является класс монотонных булевых функций, именно этот класс и исследуется в данной работе с точки зрения реализации принадлежащих ему функций схемами из функциональных элементов в трехмерном пространстве.

Несмотря на имеющиеся оценки сложности схем для различных классов функций, оценки для объемов схем практически не встречаются. Поэтому целью данной работы является установление оценок физического объема схем, построенных для класса монотонных булевых функций от n переменных — M_n. Функции из этого класса реализуются в виде схемы из функциональных элементов S_f [4] в базисе, состоящем из конъюнкторов и дизъюнкторов, а также соединяющих их проводников. Каждый конъюнктор или дизъюнктор представляет собой шар радиуса R, в который входят два проводника и один выходит. Проводники представляются цилиндрами с диаметром d. Объем схемы, обозначим его $V(n)$, построенной из этих функциональных элементов и был оценен в данной работе. Также в работе получены нижняя и верхняя оценка объема схемы, реализующей симметричные монотонные булевы функции, обозначим его $V_{sym}(n)$.

В данной работе подробно исследовано представление монотонных функций в виде:

$$f = \bigvee_i a_i \cdot b_i,$$

где $a_i \in A, b_i \in B$ и A — множество всевозможных конъюнкций от

первых $\frac{n}{2}$ переменных, а B — множество всевозможных конъюнкций от других $\frac{n}{2}$ переменных. Для такого представления функции был предложен метод построения схемы в виде параллелипипеда, найдены верхняя и нижняя оценки для объема таких схем.

Получены следующие результаты.

Теорема 1. *Имеют место при* $n \to \infty$ *соотношения:*

1)

$$C_1(R) \cdot \frac{2^n}{n^{\frac{3}{2}}} \lesssim V(n) \lesssim C_2(R,d) \cdot 2^n;$$

2) *при* $d \leq 2R$

$$\sqrt{\frac{2}{\pi}} \cdot \frac{2^n}{n^{\frac{3}{2}}} \cdot \frac{4}{3}\pi R^3 \lesssim V(n) \lesssim 16R^3 \cdot (1 + \frac{3d}{4R}) \cdot 2^n;$$

3) *при* $d > 2R$

$$\sqrt{\frac{2}{\pi}} \cdot \frac{2^n}{n^{\frac{3}{2}}} \cdot \frac{4}{3}\pi R^3 \lesssim V(n) \lesssim 2^n \cdot d^2 \cdot (4R + 3d).$$

Схемы строятся явно.

Теорема 2. $(n \log n)\frac{4}{3}\pi R^3 \leq V_{sym}(n) \leq 8 \cdot n^2 \cdot R^3$

Автор выражает благодарность за внимание, проявленное к работе, В. Б. Кудрявцеву и Н. Ю. Волкову.

Список литературы

1. Андреев А. Е. Об одном методе получения эффективных нижних оценок монотонной сложности // Алгебра и логика. — 1987. — Т. 26, № 1.

2. Угольников А. Б. О реализации монотонных функций схемами из функциональных элементов // Проблемы кибернетики, вып. 31. — 1976.

3. Лупанов О. Б. О вентильных и контактно-вентильных схемах // ДАН СССР. — 1956. — Т. 111, № 6.

4. Яблонский С. В. Введение в дискретную математику. — М.: Высшая школа, 2003.

О ДИАГНОСТИЧЕСКИХ ЭКСПЕРИМЕНТАХ С АВТОМАТАМИ И СЛОЖНОСТИ ПОРОЖДЕНИЯ ЭЛЕМЕНТОВ ПОЛУГРУПП

П. А. Пантелеев (Москва)

В знаменитой работе Э. Мура [1] было введено понятие простого диагностического эксперимента для конечного автомата, позволяющего в случае, если нам известна диаграмма автомата, но не известно начальное состояние определить после проведения эксперимента это начальное состояние. Мур рассматривал простые диагностические эксперименты двух типов: *безусловные* (сокращенно п.б.д.э.), когда подаваемая последовательность не зависит от реакции автомата и *условные* (сокращенно п.у.д.э.), когда каждый следующий подаваемый символ зависит от реакции автомата на уже поданные. Позднее, в книге А. Гилла [2] эти понятия были обобщены на произвольные подмножества состояний автомата и получены первые оценки функции Шеннона длины таких экспериментов. В работе М. Н. Соколовского [3] были установлены верхняя и нижняя оценки функции Шеннона $l(n,k)$ длины п.б.д.э. для k-элементного подмножества n-элементного множества состояний автомата.

В данной работе продолжено изучение функции $l(n,k)$. Найдена асимптотика логарифма для $l(n,k)$ при $n,k\to\infty$ и $k/n\to a\in(0,1)$. Как показал Соколовский [3], функция $l(n,k)$ тесно связана с функцией Шеннона $l(n)$ сложности порождения в худшем случае произвольного элемента в произвольном базисе из множества преобразований n-элементного множества. Получены следующие результаты.

Теорема 1. *Имеет место* $l(n)=2^n\mathrm{e}^{\sqrt{\frac{1}{2}n\ln n}(1+o(1))}$ *при* $n\to\infty$.

Теорема 2. *Имеет место* $\ln l(n,k)\sim\varphi(a)\cdot n$, *при* $n\to\infty$ *и* $k/n\to a\in(0,1)$, *где* $\varphi(a)=H(a)$ *если* $a\le 1/2$ *и* $\varphi(a)=1$ *иначе.*

Список литературы

1. Moore E. F. Gedanken-experiments on sequential machines // Automata Studies. — 1956. — P. 129–153 [русский перевод: "Автоматы" (сб. статей). — М.: ИЛ, 1956. — С. 179–210.]

2. Гилл А. Введение в теорию конечных автоматов. — М.: Наука, 1966.

3. Соколовский М. Н. Сложность порождения подстановок и эксперименты с автоматами // Методы дискретного анализа в теории кодов и схем. — 1976. — Вып. 29. — С. 68–86.

ОСОБЕННОСТИ МОДЕЛИРОВАНИЯ ГРАФИКОВ ВЕРОЯТНОСТНЫМИ ИСТОЧНИКАМИ

Д. В. Пархоменко (Москва)

Под вероятностным источником (вероятностным автоматом без входа) понимается набор $L = (Q, E, A, B, \pi)$, где Q — конечное множество состояний $q_1, , q_N$, E — конечное множество выходных символов, матрица $A = \{a_{ij}\}$, a_{ij} — это вероятность перехода из состояния q_i в состояние q_j, $1 \le i, j \le N$, $B = \{b_{ik}\}$, b_{ik} — это вероятность выдать символ ε_k в состоянии q_i, где $1 \le k \le |E|$, $\pi = \{\pi_i\}$ — вектор распределения вероятностей начального состояния, $1 \le i \le N$ [1],[2].

Вероятностный источник работает по тактам и порождает слова из E^*. Сначала, в соответствие с распределением π, выбирается начальное состояние q_i, и, в соответствии с матрицей $\{b_{ik}\}$, — выходной символ ε. В соответствии с матрицей A осуществляется переход в следующее состояние. За T тактов источник выдаст последовательность $\varepsilon = \varepsilon_1, \ldots, \varepsilon_T$.

Вероятность ее выдачи задается формулой

$$P(\varepsilon | A, B, \pi) = \sum_{Q^T} \pi_{q_1} b_{q_1}(\varepsilon_1) \prod_{s=1}^{T-1} a_{q_s q_{s+1}} b_{q_{s+1}}(\varepsilon_{s+1}), \qquad (1)$$

где Q^T — множество всех последовательностей состояний длины T, $a_{q_1 q_2} \in A$, $b_q(\varepsilon_i) \in B$.

Под обучением вероятностного источника понимается адаптивное изменение матриц A,B и вектора π.

Основная трудность, при распознавании с помощью вероятностных источников — определение числа состояний источника, способного решать поставленную задачу.

Заметим, что вероятностный источник, согласно формуле (1), задает распределение вероятностей на словах длины T, и не всякое распределение может быть задано вероятностным источником. В самом деле, после обучения источника получается вероятностное распределение, к примеру, на булевом кубе E_2^N, $E_2 = \{0, 1\}$, т. е. функция $f(x_1, \ldots, x_N) : E_2^N \to [0, 1]$, $\sum f(\sigma) = 1$, здесь суммирование ведется по всем вершинам σ булева куба. Имеет место

Замечание. *Для любого натурального k существует натуральное $N > k + 1$ и распределение $f(x_1, \ldots, x_N) : E_2^N \to [0, 1]$, такое, что не существует вероятностного источника $L = (Q, E_2, A, B, \pi)$, с k состояниями, реализующего распределение f.*

Систему вероятностных источников $\{L_i\}$ используют для распознавания через синтез. В самом деле, для каждого слова ε по формуле (1) мы знаем вероятность $P(\varepsilon|L_i)$ того, что его выдал данный вероятностный источник. Выберем в качестве результата распознавания то i, у которого $P(\varepsilon|L_i)$ максимально.

Автор применил данную методику к задаче распознавания засыпаний человека. Задача важна для определения засыпания водителей транспортных средств и авиадиспетчеров. Видеокамера снимала область, содержащую глаза испытуемого.

Полученное изображение обесцвечивалось и вычислялась ширина открытия глаза в данный момент времени. Таким образом, получалась последовательность чисел — степеней открытия глаза. По этой квантованной последовательности и надо было предсказать засыпание водителя. Связь длительности и частоты морганий с состоянием бодрствования человека описана в [7].

Для предсказания засыпания требуется точное определение числа и длительности морганий. Несмотря на кажущуюся простоту, это — непростая задача. Дело в том, что человек может по-разному держать голову во время вождения, и жестко закрепленные видеокамеры будут фиксировать различного вида сигналы, которые могут быть неправильно классифицированы. Например, если человек смотрит из-подлобья или отвел взгляд в сторону, то обычный алгоритм определения моргания по порогу — если график упал ниже порога, то фиксируем моргание — не сработает или сработает неверным образом. Также ошибки возможны при резкой смене освещения.

Обучив специальный источник K для морганий на разного рода морганиях, и специальный источник L для неморгающего глаза, получилось решающее правило: является ли поданная на вход последовательность чисел $\varepsilon = \varepsilon_1, \ldots, \varepsilon_N$ морганием будет определяться исходя из того, какая вероятность больше: $P(\varepsilon_1, \ldots, \varepsilon_N|K)$ или $P(\varepsilon_1, \ldots, \varepsilon_N|L)$. При этом длительность моргания определяется исходя из наиболее вероятной последовательности состояний $q_1, \ldots, q_N$ для данного источника с помощью алгоритма Витерби, где N — длина входной последовательности. Этот метод был реализован в программе и протестирован. Результат предсказания засыпаний — свыше 98% на качественных видеозаписях, что существенно превосходит пороговый метод определения морганий. Более того, алгоритм обнаруживает моргания, пропущенные экспертом. Подробнее эта модель описана в [6]. На основании статьи [7] о связи динамики морганий с засыпаниями, можно проверить возможность предсказания засыпания с помощью аппарата вероятностных источников.

Список литературы

1. Кудрявцев В. Б., Алешин С. В., Подколзин А. С. Введение в

теорию автоматов. — М.: Наука, 1985.
2. Бухараев Р. Г. Введение в теорию вероятностных автоматов. — М.: Наука, 1985.
3. Dempster A. P., Laird N. M., Rubin D. B. Maximum likelihood from incomplete data via the EM algorithm // J. Royal Stat. Soc. — 1977. — V. 39. — P. 1–87.
4. Music and speech detection system based on hidden Markov models and Gaussian mixture models // White paper by compure.com.
5. Левинсон С. Е. Структурные методы автоматического распознавания речи // ТИИЭР. — 1985. — № 11. — С. 100–126.
6. Baum L. E. An inequality and associated maximization technique in statistical estimation for probabilistic functions of Markov processes // Inequalities. — 1972. — V. 3. — P. 1–8.
7. Бабин Д. Н., Мазуренко И. Л., Холоденко А. Б. О перспективах создания системы автоматического распознавания слитной устной русской речи // Интеллектуальные системы. —2004. — Т. 8, вып. 1–4. — С. 45–70.
8. Пархоменко Д. В. Применение марковских моделей к проблеме распознавания засыпаний // Вопросы атомной науки и техники. — 2008. — Вып. 4. — С. 54–60.
9. Electrooculogram analysis and development of a system for defining stages of drowsiness. — Report from Linkoping University, Dept. Biomedical Engineering. LiU-IMT-EX-351.

О МОДЕЛИРОВАНИИ ПРОЦЕССОВ СРЕДСТВАМИ СИСТЕМНОЙ ДИНАМИКИ

В. И. Петренко, А. П. Рыжов (Москва)

В данной работе описывается такое направление в моделировании сложных систем как системная динамика. Это направление формализует единый подход к моделированию сложных систем, помогает упростить этот процесс и спрогнозировать поведение системы в будущем. Применения системной динамики можно найти в таких областях, как микроэлектроника, медицина, экологии и др.

Это направление было разработано Дж. Форрестером в 1960-х годах. Под системой понимается любая обособленная группа элементов, взаимодействующих во времени, которая функционирует как единое целое.

Этапы развития направления:

• Общая концепция системной динамики [1].

• Индустриальная динамика — применения концепции к моделированию систем на промышленных предприятиях [2].

• Мировая динамика. Применения в социальных системах, демографии и экологии [3].

В докладе описывается процесс моделирования в терминах системной динамики, который состоит из двух этапов.

На первом этапе определяется граница системы, набор ключевых элементов и необходимый уровень детализации. Устанавливаются взаимосвязи между элементами (как количественные и качественные значения).

На втором этапе построенная модель анализируется с помощью компьютера. Модель уточняется и корректируется. Для анализа модели используется специализированное программное обеспечение. На данном этапе проверяется выполнение ключевых свойств системы и динамика ее поведения в данной модели, вносятся финальные корректировки. В докладе приводится пример интерфейса одной из таких программ.

Далее описываются типы систем и основные элементы моделей. Системы можно разделить на закрытые и открытые. Системы первого типа не допускают вмешательства извне: фиксируются начальные значения показателей, а дальнейшее динамическое поведение системы определяется исключительно взаимосвязями внутри нее. Открытые же системы допускают вмешательство извне.

Процесс моделирования начинается с построения диаграмм процессов. Все элементы системы взаимосвязаны и образуют петли обратной связи. Их разделяют на положительные и отрицательные, в зависимости от динамического поведения значений элементов внутри них. Основными элементами диаграмм являются переменные уровней (состояний) и интенсивностей (скоростей). В докладе описываются особенности моделирования в терминах системной динамики и приводятся примеры всех вышеописанных элементов моделирования.

Приводятся следующие примеры современного применения системной динамики при моделировании:

1. Системный анализ роста ВВП.

2. Системный анализ перехода к новому поколению литографии [4].

3. Системный анализ инвестиций в технологии литографии [5].

4. Анализ рынка электроэнергии Швейцарии.

В реальных системах невозможно мгновенное получение данных и значениях элементов системы. Поэтому, при моделировании динамики систем рассматривается дискретная временная ось. Этот факт

дает возможность применить рассмотреть любую модель в терминах теории автоматов. В таком случае:

• Состояниями автомата являются закодированные состояния системы

• Входной алфавит кодирует поступающие в систему на каждом шаге решения (в случае открытых систем)

• Выходной алфавит кодирует некоторую функцию полезности, введенную для оценки принимаемых решений. Она зависит от поставленных целей

• Функции переходов и выходов определяются взаимосвязями внутри системы, которые были установлены в процессе моделирования

В докладе предлагаются возможные постановки математических задач, имеющие как теоретический, так и практический интерес.

1. Оптимизация моделей.

2. Нахождение классов входных воздействий, обеспечивающих необходимое поведение системы (стабилизацию, рост значения какого-либо элемента и т. д.)

3. Исследование устойчивости систем.

Список литературы

1. Forrester J. W. Principles of systems. — Wright-Allen Press, 1968. — С. 10–50.

2. Forrester J. W. Urban dynamics. — Pegasus Comunications, Inc., 1999. — С. 12–16.

3. Foster R. O. The dynamics of blood sugar regulation // MIT, 1970. — С. 25–30, 41.

4. Boksha V. V. Microlithography Dynamics. Social, economic, spatial and temporal implications of developments in computing technology // MIT Thesis. — M. Sc. in Management, 2000. — P. 154.

5. Boksha V. V., Bruggeman B., O'Brien M. Microlithography cost analysis // Proceedings of Interface Symposium. — San Diego, California, 1999. — P. 10.

О МАРКОВСКИХ СЛУЧАЙНЫХ ПОЛЯХ

А. А. Петюшко (Москва)

Пусть $A = \{1, 2, ..., a\}$ и $B = \{1, 2, ...b\}, a, b < \infty$ — два конечных множества. Пусть $S = \{1, 2, ..., N\}$ — множество индексов.

Пусть $X = \{X_i |\ i \in S\}$ — многомерная случайная величина, такая что каждая компонента X_j, являющаяся одномерной случайной

величиной, принимает значение x_j и определена в своем вероятностном пространстве. Для простоты будем считать, что $\forall j$ X_j дискретны, определены на одном вероятностном пространстве и множество значений — конечно.

Также для удобства можно представлять, что множество индексов S задает множество точек на плоскости. Соответственно, рассматриваем реализацию многомерной случайной величины X в этих точках. Введенная таким образом случайная величина X называется *случайным полем* (*Random Field*).

Совместное событие $(X_1 = x_1, ..., X_N = x_N)$, или кратко $X = x$, где $x = \{x_1, ..., x_N\}$, назовем *конфигурацией* X.

Пусть X — случайное поле со значениями на множестве A, т. е. $\forall i \in S$ $x_i \in A$. Если x — какая-то конкретная конфигурация X, то χ — множество всех возможных конфигураций:

$$\chi = \{x = (x_1, ..., x_N) |\ x_i \in A\ \forall i \in S\}.$$

Введем понятие *системы соседства*: это множество $\partial = \{\partial i, i \in S\}$, где ∂i — множество элементов из S, называемое *шаблоном соседства для элемента* i, такая что:

$$\begin{cases} i \notin \partial i, \\ i \in \partial j \Leftrightarrow j \in \partial i. \end{cases}$$

Определение. Случайное поле X будем называть *марковским случайным полем* (Markov Random Field, MRF) в соответствии с системой соседства ∂ тогда и только тогда, когда $\forall i$:

$$\begin{cases} P(X = x) > 0\ \forall x \in \chi, \\ P(X_i = x_i |\ X_j = x_j,\ j \in S \backslash \{i\}) = P(X_i = x_i |\ X_j = x_j,\ j \in \partial i). \end{cases}$$

Определение. *Клика* c — множество элементов из S, т.ч. $\forall s, r \in c \Rightarrow r \in \partial s$. Заметим, что любое подмножество клики — также клика.

Пусть x_c — набор значений X_i, где $i \in c$. Введем *потенциальную функцию* $V_c(x_c)$ как любую функцию от x_c.

Определение. Дискретное распределение называется *распределением Гиббса*, если

$$\mathbf{P}(X = x) = \frac{1}{Z} \exp\left(-\sum_{c \in C} V_c(x_c)\right), \tag{1}$$

где C — множество всех клик, а Z — нормирующая константа, тАкая что:

$$Z = \sum_{x \in \chi} \exp\left(- \sum_{c \in C} V_c(x_c) \right). \quad (2)$$

Наиболее важной теоремой, связывающей марковские случайные поля и распределение Гиббса, является следующая

Теорема (Hammersley—Clifford) [1]. X — *марковское случайное поле* $\Leftrightarrow$ $\mathbf{P}(X = x)$ — *распределение Гиббса.*

Таким образом, мы имеем возможность вычислять вероятность конфигурации для любого марковского случайного поля по формулам (1), (2).

Определение. *Скрытое марковское случайное поле* (Hidden Markov Random Field, HMRF) — пара случайный полей (X, Y), т.ч. выполняются следующие условия:

1) $X = \{X_i, i \in S\}$ — так называемое "скрытое" (или, другими словами, ненаблюдаемое) марковское поле со значениями в A.

2) $Y = \{Y_i, i \in S\}$ — наблюдаемое (вовсе не обязательно марковское) случайное поле со значениями в B. Важно, что $\forall i \in S, \forall d \in A$ известны условные распределения $\mathbf{P}(Y_i |\ X_i = d)$.

3) Для любой конфигурации $x \in \chi$ случайные величины Y_i условно независимы, т. е.

$$\mathbf{P}(Y |\ X = x) = \prod_{i \in S} \mathbf{P}(Y_i |\ X_i = x_i).$$

Рассмотрим марковскую цепь с состояниями $x_0, x_1, ..., x_n$, функционирующую в дискретном времени. Построим многомерную случайную величину $X = \{X_i, i = \overline{0..n}\}$ по этой марковской цепи следующим образом: $\mathbf{P}(X_i = x_i)$ — это вероятность того, что в момент времени i мы находились в состоянии x_i. Назовем X *порожденной* случайной величиной.

Теорема 1. *Любая порожденная случайная величина — это марковское случайное поле линейной структуры.*

Теорема 2. *Любое марковское случайное поле линейной структуры — это порожденная случайная величина.*

Теперь рассмотрим скрытую марковскую модель [2] и ее связь с марковским случайным полем и скрытым марковским случайным полем.

Рассмотрим скрытую марковскую модель, функционирующую в дискретном времени. Пусть при некотором ее функционировании при проходе через состояния $x_0, x_1, ..., x_n$ на выход подавались буквы $y_0, y_1, ..., y_n$ соответственно. Рассмотрим многомерную случайную величину

$$Z = (Z_1, Z_2, ..., Z_{2n+2}) = (X_0, Y_0, X_1, Y_1, ..., X_n, Y_n),$$

причем вероятность $\mathbf{P}(X_i = x_i | \ X_{i-1} = x_{i-1})$ — это вероятность перехода $a(x_{i-1}, x_i)$ из состояния x_{i-1} в состояние x_i, а вероятность $\mathbf{P}(Y_i = y_i | \ X_i = x_i)$ — это вероятность выдачи $b(y_i, x_i)$ буквы y_i в состоянии x_i. Назовем такую многомерную случайную величину *скрытой порожденной* случайной величиной.

Теорема 3. *Любая скрытая порожденная случайная величина — это скрытое случайное марковское поле линейной структуры.*

Теорема 4. *Любое скрытое марковское случайное поле линейной структуры — это скрытая порожденная случайная величина.*

Список литературы

1. Hammersley J. M., Clifford P. Markov random fields in statistics // Unpublished paper. — 1971.

2. Rabiner L. R. A tutorial on hidden Markov models and selected applications in speech recognition // Proceedings of the IEEE. — February 1989. — 77 (2). — P. 257-286.

МАТЕМАТИЧЕСКАЯ МОДЕЛЬ НЕПЕРЕЧИСЛИТЕЛЬНЫХ ЗАДАЧ ПОИСКА

А. П. Пивоваров (Москва)

Данная работа основывается на информационно-графовой модели поиска информации [1]. В этой модели перечислительная задача информационного поиска (ЗИП) представляет из себя тройку $I = \langle X, V, \rho \rangle$, где X — множество запросов, V — библиотека, являющаяся конечным подмножеством множества всех возможных записей Y, а ρ — отношение поиска, заданное на $X \times Y$. При этом содержательно задача I состоит в том, чтобы для любого произвольного запроса $x \in X$ перечислять те и только те записи из V, которые находятся в отношении ρ с x.

Однако в ряде ситуаций требуется получить не сам ответ как множество записей, но результат вычисления некоторой функции на нем. Дадим определение для описания задач такого вида.

Пятерку $S = \langle X, Y, Z, \rho, \xi \rangle$, где Z — множество ответов, $\xi : 2^Y \to Z$ — функция ответа, будем называть *типом вычислительных задач информационного поиска*. Пятерку $I = \langle X, V, Z, \rho, \xi \rangle$, где V — некоторое конечное подмножество множества Y (в дальнейшем называемое *библиотекой*), будем называть *вычислительной задачей информационного поиска* (ВЗИП) типа $S = \langle X, Y, Z, \rho, \xi \rangle$. Содержательно будем считать, что задача $I = \langle X, V, Z, \rho, \xi \rangle$ состоит в вычислении для произвольно взятого запроса $x \in X$ значения функции ξ на множестве всех тех и только тех записей из V, которые находятся в отношении ρ с запросом x, т.е. нахождении такого $z \in Z$, что $z = \xi(\{y \in V : x \rho y\})$.

Понятие информационного графа при такой постановке задачи также меняется, но незначительно — теперь листьям будут приписываться не записи из Y, а возможные ответы $z \in Z$. При этом граф должен быть таким, что любой запрос x должен доходить хотя бы до одной вершины, помеченной соответсвующим ему ответом $z \in Z$, и не доходить ни до одной вершины с другим ответом.

Теорема 1. *Пусть дана задача поиска $I = \langle X, V, \mathbb{Z}, \rho, \xi \rangle$, где $X = \{(u, v) \in [0, 1]^2 \mid u \le v\}$, $V \subseteq [0, 1]$, $|V| < \infty$, $(u, v) \rho y \Leftrightarrow u \le y \le v$, для любого $W \subseteq V$ положим $\xi(W) = |W|$. Рассмотрим базовое множество $\mathcal{F} = \langle F, \varnothing \rangle$, где F состоит из всех возможных предикатов сравнения первой и второй координаты запроса x с константами. Тогда для любого древовидного информационного графа D над базовым множеством $\mathcal{F}$, решающего задачу I справедлива оценка:*

$$Q(D) \ge k(k+1)/2,$$

где $k = |V \cap (0, 1)|$, $Q(D)$ — количество ребер в D.

Модифицируем определение информационного графа для описания алгоритмов решения ВЗИП. Для этого введем новый объект: вычислительный информационный граф (ВИГ).

В определении ВИГ используется шесть множеств: множество запросов X, множество ответов Z, множество состояний ВИГ M с выделенным элементом $m_0 \in M$, называемым *начальным состоянием* (также зафиксируем *функцию вычисления ответа по состоянию* $\sigma : M \to Z$), *множество F одноместных предикатов*, заданных на множестве X, *множество G одноместных переключателей*, заданных на множестве X (*переключатели* — это функции, область

значений которых является начальным отрезком натурального ряда), *множество H функций изменения состояния* вида $h : M \to M$, такое, что любые две функции из H коммутируют относительно операции суперпозиции. Шестерку $\mathcal{F} = \langle F, G, H, M, m_0, \sigma \rangle$ будем называть *базовым множеством* .

Определим ВИГ с точки зрения его структуры. Пусть нам дана ориентированная многополюсная сеть. Выделим в ней один полюс и назовем его *корнем*, а остальные полюса назовем *листьями*.

Выделим в сети некоторые вершины и назовем их *точками переключения* (полюса могут быть точками переключения). Каждой точке переключения β сопоставим некий символ из G. Если β — вершина сети, то через ψ_β обозначим *полустепень исхода* вершины β. Для каждой точки переключения β ребрам, из нее исходящим, поставим во взаимно однозначное соответствие числа из множества $\{\overline{1, \psi_\beta}\}$. Эти ребра назовем *переключательными*.

Ребра, не являющиеся переключательными, назовем *предикатными*. Каждому предикатному ребру сопоставим некоторый символ из множества F. Сопоставим каждому листу сети некоторый символ из множества H. Это соответствие назовем *нагрузкой листьев*. Полученную нагруженную сеть назовем *вычислительным информационным графом* (ВИГ) над базовым множеством $\mathcal{F} = \langle F, G, H, M, m_0, \sigma \rangle$.

Определим функционирование ВИГ. Скажем, что предикатное ребро проводит запрос $x \in X$, если предикат, приписанный этому ребру, принимает значение 1 на запросе x; переключательное ребро, которому приписан номер n, проводит запрос x, если переключатель, приписанный началу этого ребра, принимает значение n на запросе x; ориентированная цепочка ребер проводит запрос x, если каждое ребро цепочки проводит запрос x; запрос x проходит в вершину β ВИГ, если существует ориентированная цепочка, ведущая из корня в вершину β, которая проводит запрос x. Если $\alpha_1, \ldots, \alpha_p$ — множество всех листьев ВИГ таких, что запрос проходит в эти листья, то будем называть *конечным состоянием ВИГ U на запросе x* состояние $m_U(x) = h_1 \ldots h_p(m_0)$, где h_i — нагрузка листа α_i $(i = 1, \ldots, p)$. В случае, когда запрос x не проходит ни в один лист ВИГ, будем считать, что $m_U(x) = m_0$. *Ответом ВИГ U на запрос x* назовем $z_U(x) = \sigma(m_U(x))$. Эту функцию $z_U(x) : X \to Z$ будем считать результатом функционирования ВИГ U и называть *функцией ответа*.

Объемом $Q(U)$ ВИГ U назовем число ребер в ВИГ U. Эта величина характеризует объем памяти, требуемый для реализации алгоритма поиска, задаваемого ВИГ U. *Сложностью ВИГ U на за-*

просе x назовем число $T(U,x)$, равное сумме числа переключателей и предикатов, вычисленных в процессе обработки запроса x. *Верхней сложностью* называют величину $\hat{T}(U) = \sup_{x \in X} T(U,x)$.

Пусть нам дана ВЗИП $I = \langle X, V, Z, \rho, \xi \rangle$. Скажем, что ВИГ U *решает* ВЗИП $I = \langle X, V, Z, \rho, \xi \rangle$, если $z_U(x) = \xi(\{y \in V : x \rho y\})$ для любого запроса $x \in X$.

Рассмотрим ту же задачу информационного поиска I, что и в теореме 1. Рассмотрим базовое множество $\mathcal{F} = \langle F, G, H, M, m_0, \sigma \rangle$, где F состоит из всех возможных предикатов сравнения первой и второй координаты запроса x с константами и тождественно единичного предиката, $G = \varnothing$, $M = \mathbb{Z}, m_0 = 0$, $H = \{h_a : M \to M \mid a \in \mathbb{Z}\}$, где $h_a(m) = m + a$, $\sigma(m) = m$.

Теорема 2. *Существует ВИГ U над базовым множеством $\mathcal{F}$, такой что U разрешает ВЗИП I и имеет следующие характеристики:* $\hat{T}(U) \leq 4]\log_2(|V|+1)[+2$, $Q(U) = 4|V| + 2$.

Автор выражает благодарность профессору Э. Э. Гасанову за постановку задачи и помощь в работе.

Список литературы

1. Гасанов Э. Э., Кудрявцев В. Б. Теория хранения и поиска информации — М.: Физматлит, 2002

О СУЩЕСТВОВАНИИ АЛГОРИТМА ДЛЯ РАЗРЕШИМОСТИ ЗАДАЧИ ОБ А-ПОЛНОТЕ ДЛЯ СИСТЕМ Д.ФУНКЦИЙ, СОДЕРЖАЩИХ ВСЕ ОДНОМЕСТНЫЕ S-О.-Д.ФУНКЦИИ

М. А. Подколзина (Москва)

Пусть E_2^∞ — множество бесконечных последовательностей, составленных из 0 и 1. Пусть $P_{\text{О.Д.}}$ — множество всех о.-д. функций, переменные которых принимают значения из E_2^∞. Будем считать, что на множестве $P_{\text{О.Д.}}$ заданы операции суперпозиции [1].

Множество $\mathfrak{M}$, $\mathfrak{M} \subseteq P_{\text{О.Д.}}$, называется А-полным, если для любой о.-д. функции f и для всякого $\tau \geq 1$ из о.-д.функций множества $\mathfrak{M}$ с помощью операции суперпозиции можно получить о.-д. функцию g, совпадающую с f на словах длины τ [2].

Известно [3], что не существует алгоритма для распознавания А-полноты конечных множеств о.-д. функций.

Пусть $S(P^2_{\text{о.д.}}(1))$ — множество всех о.-д. функций, зависящих от одной переменной и не выпускающих ни одного значения из множества E_2^∞ [4].

Пусть N — множество всех таких систем $\mathfrak{M}$ из $P^2_{\text{о.д.}}$, что $S(P^2_{\text{о.д.}}(1)) \subset \mathfrak{M}$ и множество $\mathfrak{M} \setminus S(P^2_{\text{о.д.}}(1))$ конечно [5].

Имеет место

Теорема. *Существует алгоритм для распознавания A-полноты систем о.-д. функций, принадлежащих множеству* N.

Список литературы

1. Кудрявцев В. Б., Алешин С. В., Подколзин А. С. Введение в теорию автоматов. — М.: Наука, 1985.

2. Буевич В. А. Условия A-полноты для конечных автоматов. Ч. 1. М.: Изд-во МГУ, 1986.

3. Буевич В. А. Об алгоритмической неразрешимости распознавания A-полноты для ограниченно-детерминированных функций // Математические заметки. — 1972. — Т. 6. — С. 687–697.

4. Буевич В. А., Подколзина М. А. Критерий полноты S-множеств детерминированных функций // Математические вопросы кибернетики. Вып. 16. — М.: Физматлит, 2007. — С. 191–238.

5. Буевич В. А., Клиндукова Т. Э. О существовании алгоритма для распознавания A-полноты систем, содержащих все одноместные ограниченно-детерминированные функции // Математические вопросы кибернетики. Вып. 8. — М.: Наука, 1999. — С. 289–297.

АЛГЕБРАИЧЕСКИЕ МОДЕЛИ ПРОГРАММ И ЭКВИВАЛЕНТНЫЕ ПРЕОБРАЗОВАНИЯ В НИХ

Р. И. Подловченко (Москва)

Рассматриваемые нами алгебраические модели программ введены в [1] как обобщение существующих к тому времени моделей программ двух типов: предложенных А. А. Ляпуновым и Ю. И. Яновым в [2] и В. М. Глушковым и А. А. Летичевским в [3]. Как и другие модели программ, алгебраические предназначены для исследования семантических свойств программ, взятых в определенной формализации. При таком исследовании основными являются следующие вопросы:

— как установить, что две программы функционально эквивалентны, т. е. реализуют одну и ту же функцию;

— какими преобразованиями программа переводится в любую ей эквивалентную.

Привлекательность алгебраических моделей программ обусловлена следующими их характеристиками:

— модели построены для формализованных программ, которые, по существу, совпадают с разделами операторов в реальных программах, записанных на алгоритмических языках типа Паскаль; этим они пригодны для изучения семантических свойств реальных последовательных программ;

— структуры объектов модели, называемых схемами программ, берутся совпадающими со структурами моделируемых программ; поэтому всякое структурное преобразование схемы программ одновременно является структурным преобразованием программы, для которой построена эта схема;

— имеются удобные достаточные признаки того, что выбранная алгебраическая модель программ является аппроксимирующей, т. е. существует класс программ такой, что из эквивалентности схем программ, принадлежащих модели, следует функциональная эквивалентность программ из этого класса, моделируемых данными схемами; для аппроксимирующей модели всякое эквивалентное преобразование структуры ее схемы является эквивалентным преобразованием структуры моделируемой схемой программы из аппроксимируемого класса программ.

В проблематике теории алгебраических моделей основными считаются две проблемы: проблема эквивалентности схем в модели и проблема эквивалентных преобразований (э. п.) в модели. Первая состоит в поиске алгоритма, который, получив на свой вход две произвольные схемы из модели, устанавливает, эквивалентны они или нет. Вторая проблема заключается в построении системы э. п., полной в модели, т. е. обладающей свойством: какими бы ни были две эквивалентные схемы из модели, существует конечная цепочка преобразований, принадлежащих системе, транслирующая первую схему во вторую. Проблема э. п. в модели всегда обсуждается в случае, когда в модели разрешима проблема эквивалентности схем. Здесь предметом рассмотрений являются так называемые уравновешенные полугрупповые модели программ с левым сокращением — достаточно широкое подмножество алгебраических моделей программ. Их выбор обусловлен двумя факторами: они являются аппроксимирующими, и в них разрешима проблема эквивалентности; последнее установлено в [4], приемлемые по сложности разрешающие алгоритмы описаны в [5]. Основная задача данной работы состоит в решении для рассматриваемых моделей проблемы э. п., т. е. в построении для них полных систем э. п.

Решение проблемы э.п. ищется в заранее очерченном множестве

так называемых фрагментных преобразований схем. Для этого вводится понятие фрагмента схемы, определяется отношение эквивалентности фрагментов и описывается операция подстановки в схеме вместо принадлежащего ей фрагмента другого согласованного с ним фрагмента. Операция подстановки при ее выполнении осуществляет преобразование схемы, называемое фрагментным. Оно является эквивалентным, если эквивалентны участвующие в операции фрагменты. Допустимыми при решении проблемы э. п. объявляются системы фрагментных э. п., заданные конечным числом множеств, которые состоят из пар эквивалентных фрагментов. Эти множества обязаны быть разрешимыми, т. е. сопровождаемыми алгоритмами, устанавливающими принадлежность множеству той или иной пары фрагментов. Множества именуются аксиомами.

Доказательство полноты системы в модели проводится традиционным способом, а именно: описывается алгоритм, который, получив на свой вход две эквивалентные схемы из модели, транслирует их к общему виду, т. е. в изоморфные схемы; выполняемые этим алгоритмом фрагментные преобразования схем подсказывают введение необходимых аксиом.

Основным результатом данной работы является построение систем фрагментных э.п. схем, полных в рассматриваемых моделях программ, для каждой модели — своей системы. Применяемые фрагментные преобразования схем программ основаны на построении следующего алгоритма. Пусть G_1, G_2 — эквивалентные схемы, принадлежащие рассматриваемой модели. Сначала каждая схема G_i, $i = 1, 2$, трансформируется в эквивалентную ей матричную схему G_i''. Далее используются структурные свойства эквивалентных схем, установленные в [4]. В схеме G_i', $i = 1, 2$, непременно имеются фрагменты, именуемые кустами. Осуществляется преобразование G_i' в эквивалентную ей схему G_i'', $i = 1, 2$, в которой всякий принадлежащий ей куст является чистым, т. е. имеет единственный вход.

Согласно [4, 5], в эквивалентных схемах G_1'', G_2'' между входящими в них кустами имеется соответствие. Последующие трансформации этих схем состоят в замене во всякой паре соответствующих друг другу чистых кустов самих кустов одинаковыми цепочками операторов. Полученные таким образом схемы G_1''', G_2''' являются не просто эквивалентными, а строго эквивалентными, т.е. эквивалентными как обычные конечные автоматы.Каждая из схем G_1''', G_2''' трансформируется в схему, подобную минимальному автомату, что и приводит к изоморфным схемам. Подсказанные построенным алгоритмом преобразования слагаются в систему, описываемую семью аксиомами.

Список литературы

1. Подловченко Р. И. Иерархия моделей программ // Программирование. — 1981. — № 2. — С. 3–14.

2. Янов Ю. И. О логических схемах алгоритмов // Проблемы кибернетики. — 1958. — Вып. 1. — С. 75–127.

3. Глушков В. М., Летичевский А. А. Теория дискретных преобразователей // Избранные вопросы алгебры и логики. — 1973. — С. 5–39.

4. Подловченко Р. И. Техника следов в разрешении проблемы эквивалентности в алгебраических моделях программ // Кибернетика и системный анализ. — 2009. — № 5. — С. 25–37.

5. Подловченко Р. И. К вопросу о полиномиальной разрешимости проблемы эквивалентности в алгебраических моделях программ // Кибернетика и системный анализ. — В печати.

НЕЛИНЕЙНАЯ СЛОЖНОСТЬ НЕЙРОННЫХ СХЕМ

В. С. Половников (Москва)

В работах [1, 2] была доказана теорема о том, что для любой нейронной схемы без памяти существует эквивалентная ей схема, нелинейной глубины не более двух. Так же показано, что существуют кусочно-линейные функции для реализации которых нейронными схемами единичной нелинейной глубины не достаточно. Подробнее о схемах нелинейной глубины 1 изложено в [3]. В докладе рассматриваются кусочно-параллельные функции [4], реализуемые нейронными схемами без памяти и без использования элемента F. Пусть $f(x_1, \ldots, x_n)$ — произвольная кусочно-параллельная функция в R^n, заданная k гиперплоскостями. Согласно [4], существует S — нейронная схема указанного вида нелинейной глубины два (специального вида), реализующая f. Через $L(S)$ обозначим число нелинейных элементов (θ) в схеме S, то есть нелинейную сложность S. Соответственно определим $L(f) = \min L(S)$, где минимум берется по всем нейронным схемам специального вида, реализующим f. Функция Шеннона $L(k) = \max L(f)$, по всем кусочно-параллельным функциям f, заданным k гиперплоскостями. В докладе показывается схема нахождения порядка и асимптотики функции Шеннона

$$L(k) \sim \frac{2^n}{n!}k^n,\ k \to \infty,\ n = const,\ n > 1.$$

Список литературы

1. Половников В. С. О некоторых характеристиках нейронных схем // Вестн. Моск. ун-та. Сер. 1. Математика. Механика. — 2004. — № 5. — С. 65–67.
2. Половников В. С. О некоторых характеристиках нейронных схем // Интеллектуальные системы. — 2004. — Т. 8, вып. 1–4. — С. 121–145.
3. Половников В. С. Критерий нелинейной однослойности нейронных схем // Вестн. Моск. ун-та. Сер. 1. Математика. Механика. — 2006. — № 6. — С. 3–5.
4. Половников В. С. О задаче проверки функциональной полноты в классе кусочно-параллельных функций // Вестн. Моск. ун-та. Сер. 1. Математика. Механика. — 2008. — № 6.

КРИПТОСИСТЕМА С ОТКРЫТЫМ КЛЮЧОМ НА ОСНОВЕ ЗАДАЧИ ОБ F-ВЫПОЛНИМОСТИ БУЛЕВЫХ ФОРМУЛ

Е. А. Поцелуевская (Москва)

В современном мире значительная часть информации обрабатывается в электронном виде. В связи с необходимостью обеспечить защиту такой информации при передаче по открытым каналам связи, широкое распространение получили криптографические системы с открытым ключом, основанные на различных NP-полных задачах. В настоящей работе рассматривается реализация асимметричной криптографической системы на основе NP-полной задачи об F-выполнимости булевых формул.

Задача об F-выполнимости булевых формул ставится следующим образом. Пусть $\mathbf{F} = \{F_1, \ldots, F_s\}$ — любое конечное множество формул. Определим F-формулу как конъюнкцию $F_{i_1}(\cdot)F_{i_2}(\cdot)\ldots F_{i_t}(\cdot)$ с переменными $x_1, \ldots, x_n$, расставленными некоторым образом. Проблема F-выполнимости — это проблема выполнимости F-формул. В общем случае данная задача является NP-полной.

В случае, если F-формула задана в конъюнктивной нормальной форме и каждая из функций F_i зависит не более чем от трех переменных, для решения задачи F-выполнимости существует алгоритм, приведенный в статье 1. Алгоритм основан на переборе минимального подмножества S переменных x_i, которые покрывают все дизъюнкции от трех переменных, входящие КНФ, и решении для

каждого фиксированного набора значений переменных из S полиномиальной подзадачи о 2-выполнимости.

Сложность данного алгоритма составляет $\left(1+\sum_{i=1}^{k} 2^{|S_i|}\right) poly(|x|)$, где $|x|$ — длина входа, множества S_i — это множества переменных, вычисляемые в ходе работы алгоритма, для которых выполнено: $S = \bigsqcup_{i=1}^{k} S_i$. В случае если для всех $i = 1..k$ $|S_i| \leq \log_2(poly(|x|))$ сложность алгоритма будет полиномиальной величиной.

Формирование ключевой пары. Основным параметром криптосистемы с открытым ключом на основе задачи об F-выполнимости служит количество различных переменных n, задействованных в F-формуле.

Для формирования ключевой пары рассматриваются n булевых функций $F_1, \ldots, F_n$, каждая из которых зависит не более чем от трех переменных, таких, что они определяют подстановку, и решение задачи об F-выполнимости для данного набора функций с помощью алгоритма из 1 занимает полиномиальное время.

Далее каждая из выбранных функций $F_1, \ldots, F_n$ записывается в форме полинома Жегалкина, и осуществляется замена переменных $y = Ax + b$, где $y = (y_1, \ldots, y_n)^T$, $x = (x_1, \ldots, x_n)^T$ — столбцы переменных, A — невырожденная матрица размера $n \times n$, $a_{i,j} \in \{0,1\}, i \in \{1, \ldots, n\}, j \in \{1, \ldots, n\}$, $b = (b_1, \ldots, b_n)^T$, $b_i \in \{0,1\}, i \in \{1, \ldots, n\}$. Расширенная матрица этой системы $P = (A|b)$ размера $n \times (n+1)$ будет служить закрытым ключом криптосистемы. Длина закрытого ключа равна $n^2 + n$ бит.

С функциями, полученными в ходе описанных действий, осуществляется дополнительное преобразование, зависящее только от матрицы A, в результате которого получается набор функций $h_1, \ldots, h_n$, которые представляют собой полиномы Жегалкина степени не выше 2 и зависят от набора из $2n$ переменных. Данный набор функций, закодированный значениями коэффициентов полиномов, служит открытым ключом системы. Длина открытого ключа составляет $n(n^2 + n + 1)$.

Шифрование. Шифрование осуществляется путем разбиения исходного текста на блоки длины n^2 и присваивания значений, соответствующих битам исходного текста, переменным в формулах открытого ключа получателя $h_1, \ldots, h_n$. В результате каждый блок исходного текста длины n^2 однозначным образом преобразуется в блок шифротекста длины n^2 за линейное время.

Расшифрование. Зашифрованное сообщение разбивается на блоки длины n^2. Осуществив обратное преобразование формул и пе-

ременных открытого ключа $h_1, \ldots, h_n$ с помощью своего закрытого ключа, получатель приходит к исходной системе формул $F_1, \ldots, F_n$. Из полученной системы уравнений составляется F-формула, для которой решается задача об F-выполнимости. Решение задачи занимает полиномиальное время в соответствии с исходным выбором формул. В результате получатель однозначным образом вычисляет для каждого блока шифротекста длины n^2 блок исходного текста длины n^2.

Оценка надежности криптосистемы. Для нахождения открытого текста при заданном шифротексте и открытом ключе, злоумышленнику требуется решить задачу F-выполнимости, которая NP-полна и сводится к перебору n^2 значений, либо определить исходные функции $F_1, \ldots, F_n$. Однако без знания закрытого ключа вычисление исходной системы функций также сводится к перебору. Таким образом, взлом криптографической системы потребует 2^{n^2} операций.

На текущий момент в используемых на практике криптосистемах с открытым ключом используется длина закрытого ключа в 256 бит. Для обеспечения аналогичного уровня криптостойкости в криптосистеме на основе задачи F-выполнимости достаточно задать параметр $n = 16$. В этом случае длины ключей будут следующими: длина закрытого ключа — 272 бита, длина открытого ключа — 4368 бит.

Для сокращения длины открытого ключа может быть использована следующая модификация исходной криптосистемы, где для преобразования переменных используется невырожденная матрица, такая что каждая из переменных x_i ($i \in \{1, \ldots, n\}$) зависит не более чем от двух переменных y_k ($k \in \{1, \ldots, n\}$). Тогда закрытый ключа может быть закодирован $n(4 \log_2 n + 1)$ битами, а открытый ключ может быть записан $n(12 \log_2 n + 37)$ битами. В частности, при параметре $n = 16$ длина закрытого ключа составит 272 бита, длина открытого ключа — 1360 бит.

Автор работы выражает признательность В. А. Носову за научное руководство.

Список литературы

1. Поцелуевская Е. А. Полиномиальные случаи решения задачи об F-выполнимости булевых формул // Интеллектуальные системы. — 2008. — Т. 12.

2. Алексеев В. Б., Носов В. А. NP-полные задачи и их полиномиальные варианты. Обзор // Обозрение прикладной и промышленной математики. — 1997. — Т. 4, вып. 2. — С. 165–193.

3. Schaefer T. J. The complexity of satisfiability problems // Proceed-

ings of the 10th ACM Symposium on Theory of Computing. — 1978. — P. 216–226.

ОБ ОДНОЙ ОСОБЕННОСТИ ДВУМЕРНОЙ ЗАДАЧИ О РЮКЗАКЕ

В. В. Псиола (Москва)

Существует известная оптимизационная задача "о рюкзаке", которая может быть сформулирована следующим образом: *задано конечное множество U "предметов" и для каждого из $u \in U$ "размер" $s(u) \in Z^+$ и стоимость $v(u) \in Z^+$, а так же положительное число $B \geq \max\{s(u) : u \in U\}$ — "емкость рюкзака". Требуется найти такое подмножество $U' \subseteq U$, что $\sum_{u \in U'} s(u) \leq B$ и величина $\sum_{u \in U'} v(u)$ принимает наибольшее возможное значение.*

Для рациональных значений размеров эта задача относятся к классу NP-полных [3] и это означает, что любой алгоритма нахождения наилучшего решения будет иметь экспоненциальную сложность. То есть время его работы будет сравнимо со временем полного перебора всех вариантов упаковки предметов в рюкзак и выбора наилучшего. При этом каждый вариант упаковки однозначно определяется некоторым подмножеством предметов.

Часто возникает необходимость решения 2-мерного аналога этой задачи, например, при оптимизации раскроя материалов или расстановке предметов в транспортных средствах. Постановка задачи в 2-мерном случае не так однозначна: возникает вопрос конфигурации контейнера ("рюкзака") и предметов, которые в общем случае могут быть заданы произвольными 2-мерными фигурами, а так же неоднозначности требований к расстановке предметов в контейнере. Для простоты можно ограничится рассмотрением случая прямоугольного контейнера и предметов, для которых допустима любая расстановка без пересечений друг с другом такая, что ребра предметов параллельны ребрам контейнера. Даже при таком ограничении 2-мерная задача заведомо не проще своего одномерного аналога и методы её решения востребованы.

На практике для решения 2- и 3-мерных задач "о рюкзаке" обычно используются алгоритмы быстрого нахождения приближенного решения [1, 2], но вопрос поиска наилучшего решения полным перебором тоже актуален при небольшом количестве предметов. Однако, в 2-мерном случае непонятно как именно может быть организован

переборный процесс, ведь тут, в отличии от одномерного, решение задачи определяется не только подмножеством предметов, но и их позициями в контейнере. Возможна ситуация, когда суммарная площадь предметов подмножества меньше площади контейнера, но их расстановка без пересечений невозможна. Фактически для рациональных значений линейных размеров существует бесконечное количество вариантов расстановки предметов и соответственно время полного перебора этих вариантов тоже будет бесконечно. Таким образом становится актуальным вопрос возможности организации конечного переборного процесса для нахождения наилучшего решения 2-мерной задачи "о рюкзаке".

Оказывается существует алгоритм $\widetilde{P_{2d}}$ нахождения наилучшего решения 2-мерной задачи о рюкзаке, время работы которого зависит только от количества предметов и не зависит от характеристик линейных размеров:

- перебираются все последовательности предметов в постановке задачи;
- для каждой последовательности предметов рассматривается следующее множество их расстановок:
  - первый предмет последовательности может быть установлен так, что его нижний левый угол находиться в нижнем левом углу контейнера (возможны две такие позиции);
  - для каждого следующего предмета рассматриваются все точки пересечения прямых, проходящих через ребра контейнеров или ранее установленных предметов;
  - и для каждой такой точки рассматриваются два варианта установки очередного предмета, когда его ребра параллельны ребрам контейнера, левый нижний угол совпадает с этой точкой и при этом предмет не выходит за пределы контейнера и не пересекается с ранее установленными предметами.
- таким образом для каждой позиции очередного предмета перебирается всё дерево вариантов позиций оставшихся предметов;
- среди всех рассмотренных вариантов расстановок в качестве решения задачи выбирается та, у которой суммарное значение стоимости установленных предметов максимально.

Теорема. *Алгоритм $\widetilde{P_{2d}}$ находит наилучшее решение "2-мерной задачи о рюкзаке".*

Для доказательства теоремы необходимо показать, что для любой расстановки предметов, существует их связная расстановка, у которой левый нижний угол каждого предмета находится в точке пересечения прямых, проходящий через ребра контейнера или других предметов и при этом один из предметов расположен в нижним левом углу контейнера. Чтобы это показать, достаточно все предметы из текущих позиций сместить вниз и влево "до упора" в границу контейнера или другой предмет, и таким образом получиться "связная" расстановка этих же предметов. Определенную сложность вызывает доказательство невозможности цикла позиций предметов, в котором каждая из позиций "упирается" в следующую. Это делается путём подробного анализа замкнутой прямоугольной ориентированной ломаной, которую создавала бы граница такого цикла связных предметов. Из условия того, что каждый предмет цикла соприкасается со следующим своим левым или нижним ребром можно прийти к невозможности существования такой ломаной.

К сожалению, сделанное утверждение невозможно явным образом распространить на 3-мерный случай. За счёт выхода в третье измерение там возможно существование такого цикла, а значит простое смещение позиций вниз и влево может не привести к связной расстановке. Более того в 3-мерном случае можно построить контрпример — расстановку предметов в которой позиции существенно зависят от их линейных размеров и не существует никакой другой расстановки этих же предметов. Это говорит о том, что вопрос построения подобного алгоритма в 3-х мерном случае достаточно сложен и остаётся открытым.

Список литературы

1. Псиола В. В. О приближенном решении 3-х мерной задачи об упаковке на основе эвристик // Интеллектуальные системы. — 2007. — Т. 11, вып. 1–4. — 2007. С. 83–101.

2. Псиола В. В. Оценки качества работы алгоритма Packer3d (теория и практика) // МГУ им. М. В. Ломоносова, Москва, 2009. — Деп. в ВИНИТИ 01.04.09, 182-В2009.

3. Гэри М., Джонсон Д. Вычислительные машины и труднорешаемые задачи. — М.: Мир, 1982.

О СУЩЕСТВОВАНИИ АЛГОРИТМОВ ДЛЯ РАСПОЗНАВАНИЯ ПОЛНОТЫ СИСТЕМ О.-Д. ФУНКЦИЙ ИЗ МНОЖЕСТВА N_D

А. А. Родин (Москва)

Пусть E_2^∞ — множество всех бесконечных последовательностей, составленных из 0 и 1. Пусть P — множество о.-д. функций, переменные которых принимают значения из множества E_2^∞. Будем считать, что на множестве P заданы операции суперпозиции и обратной связи. Пусть $M \subseteq P$. Замыкание множества M относительно этих операций будем обозначать через $[M]$. Известно [2], что не существует алгоритма для распознавания полноты конечных систем из P и, кроме того, в полученной функциональной системе континуум предполных классов. Более того, как показано в [3], для всякого замкнутого D из диаграммы Поста, существует континуум предполных классов, каждый из которых содержит множество P_D — множество всех о.-д. функций, в каждом состоянии которых реализуется функция из D. В связи с этим для всякого D интерес представляет следующая задача.

Пусть N_D — совокупность систем о.-д. функций M таких, что $P_D \subseteq M$, а множество $M \setminus P_D$ конечно. Существует ли алгоритм для распознавании полноты систем из N_D?

Теорема. *Существует алгоритм для распознавания полноты систем о.-д. функций из N_D, если D содержит константу* (0 *или* 1) *и тождественную функцию алгебры логики.*

Заметим, что в [4] аналогичная теорема была доказана для случая, когда $D = \{x, \overline{x}, 0, 1\}$

Список литературы

1. Кудрявцев В. Б., Алешин С. В., Подколзин А. С. Введение в теорию автоматов. — М.: Наука, 1985.

2. Кудрявцев В. Б. О мощности множеств предполных множеств некоторой функциональной системы, связанной с автоматами. — Проблемы кибернетики. Вып. 13. — М.: Физматгиз, 1965.

3. Родин А. А. О предполных классах во множестве автоматных отображений // Современные проблемы математики и их приложений. Материалы конференции, посвященной 70-летию академика В. А. Садовничего. — М.: Изд-во МГУ, 2009. — С. 372.

4. Алешин С. В. Über ein Vollständigkeits kriterium für Automatenabbildungen beruglich der Superposition // Rostoker Math. Kolloq. — 1977. — № 5. — S. 119–132.

ИНВАРИАНТНЫЕ СВОЙСТВА КОДИРОВАНИЙ СОСТОЯНИЙ АВТОМАТОВ

С. Б. Родин (Москва)

Определение 1. Нумерованной переходной системой назовем тройку (A, Q, φ), где A — входной алфавит, $Q = \{0...n-1\}$, φ — функция переходов.

В работе изучаются нумерованные переходные системы с входным алфавитом $A = E_2$ и числом состояний $n = 2^k$.

Определение 2. Кодированием множества $Q = \{0...n-1\}$ назовем взаимооднозначное отображение $F : \{0...n-1\} \to {E_2}^k$.

Каждое кодирование F для переходной системы на множестве Q порождает булевский оператор [1] $\phi : {E_2}^{k+1} \to {E_2}^k$, где

$$\phi(a, \alpha_1, ..., \alpha_k) = F(\varphi(a, F^{-1}(\alpha_1, ..., \alpha_k))), a \in A, \alpha_i \in E_2.$$

В данной работе изучался вопрос, когда кодирование приводит к набору линейных булевских функций.

Выделим из всех кодирований "стандартное" кодирование.

Определение 3. Кодирование $F_0 : \{0...n-1\} \to {E_2}^k$ назовем стандартным, если код элемента есть его двоичное представление.

Каждому кодированию F можно сопоставить перестановку s_F на множестве $F : \{0...n-1\}$ по правилу $s_F(i) = {F_0}^{-1}(F(i))$. Поскольку $n = 2^k$, то подстановки на множестве $Q = \{0...n-1\}$ могут быть представлены как многочлены над полем Галуа F_{2^k} [2]. Обозначим через P_n множество подстановок на множестве E_n. Обозначим через H_+ перестановки соответствующие многочленам $x + c$ над полем Галуа F_n, где $c \in E_n$ — константа. Обозначим через $H_L = \{s \in P_n$, такие что $\forall h \in H_+ \; \exists h' \in H_+, hs = sh'\}$.

Теорема 1. *Подстановкам, представляемым многочленами над полем Галуа F_n, являющимися линейными комбинациями над $< x^{2^i}, c >$, $i \in \{0...k\}$, $c \in E_n$ — константа, при стандартном кодировании соответствует линейный оператор.*

Каждое кодирование F на множестве Q для подстановки s порождает булевский оператор [1] $\phi : {E_2}^k \to {E_2}^k$, где

$$\hat{s}(\alpha_1, ..., \alpha_k) = F(s(F^{-1}(\alpha_1, ..., \alpha_k))), \alpha_i \in E_2.$$

Теорема 2. *Оператор, соответствующий подстановке s при стандартном кодировании, линеен тогда и только тогда, когда $s \in H_L$.*

Теорема 3. *Пусть s_0, s_1 — порождающие внутренней полугруппы переходной системы. Переходная система имеет линейную реализацию тогда и только тогда, когда $\exists$ кодирование F, такое что, а) ${s_F}^{-1} \cdot s_0 \cdot s_F$, ${s_F}^{-1} \cdot s_1 \cdot s_F$ принадлежат H_L; б) ${s_F}^{-1} \cdot s_0 \cdot s_F$, ${s_F}^{-1} \cdot s_1 \cdot s_F$ одному правому классу смежности P_n по H_+.*

Список литературы

1. Родин С. Б. Переходные системы с максимальной вариантностью относительно кодирования состояний // Интеллектуальные системы. — 1999. — Т. 4, вып. 3–4. — С. 335–352.

2. Яблонский С. В. Введение в дискретную математику — М.: Наука, 1979.

ОЦЕНКА И МОНИТОРИНГ СЛОЖНЫХ ПРОЦЕССОВ СРЕДСТВАМИ ТЕОРИИ НЕЧЕТКИХ МНОЖЕСТВ

А. П. Рыжов (Москва)

В работе описывается технология информационного мониторинга сложных процессов, разрабатываемая автором с конца 80-х — начала 90-х годов. Приводится содержательная постановка проблемы информационного мониторинга, описываются технологические и математические аспекты разработки систем информационного мониторинга.

Многие процессы в бизнесе, экономике, политике и других областях, называемых слабо (или плохо) формализуемыми, не возможно представить в виде набора уравнений, автоматов и других математических средств представления и анализа динамических систем, однако специалисты как-то решают задачи оценки состояния процесса и управления им. В общем виде задача заключается в оценке текущего состояния процесса на основе всей доступной информации, построении прогнозов его развития и выработке рекомендаций по управлению исходя из целей, стоящих перед специалистом. В работе приводятся примеры таких задач из политологии, маркетинга, финансового анализа, страхового дела. В качестве примера процессов, не являющихся таковыми, можно привести взаимодействие двух тел или распространение колебаний в однородной среде. Имеются математические модели таких процессов, информация измерима и доступна, результат можно вычислить для любого момента времени.

Будем называть задачу оценки текущего состояния системы (процесса) и построении прогнозов ее развития задачей информационного мониторинга, а человеко-компьютерные системы, обеспечивающие аналитическую поддержку подобного рода информационных задач, системами информационного мониторинга. Основными элементами систем информационного мониторинга являются информационное пространство и аналитик. В работе анализируются свойства информационного пространства: разнородность, фрагментарность, разноуровневость и ненадежность доступной информации, ее противоречивость и изменяемость во времени.

Приводятся архитектурные и технологические особенности компьютерных систем, обеспечивающие обработку такого рода информации [1]. В частности:

— для реализации возможности обработки информации из разнородных источников, в базе данных системы хранятся как сами документы, так и ссылки на них с оценкой содержащейся в них информации, данной экспертом;

— для возможности обработки фрагментарной информации используется модель процесса в виде графа;

— обработка разноуровневой информации достигается за счет предоставления пользователю возможности отнести оценку конкретного информационного материала к разным вершинам модели;

— обработка информации различной степени надежности и обладающей возможной противоречивостью или тенденциозностью достигается за счет использования лингвистических оценок экспертами данной информации;

— изменяемость во времени учитывается фиксацией даты поступления информации при оценке конкретного материала, т.е. время является одним из элементов описания объектов системы.

Для эффективного практического применения предложенных технологических решений необходима проработка ряда теоретических проблем, результаты которой приводятся в докладе. Рассматриваются три такие проблемы.

Проблема 1. Можно ли, учитывая некоторые особенности восприятия человеком объектов реального мира и их описания, сформулировать правило выбора оптимального множества значений признаков, по которым описываются эти объекты? Возможны два критерия оптимальности:

Критерий 1. Под оптимальными понимаются такие множества значений, используя которые человек испытывает минимальную неопределенность при описании объектов.

Критерий 2. Если объект описывается некоторым количеством экспертов, то под оптимальными понимаются такие множества значений, которые обеспечивают минимальную степень рассогласова-

ния описаний.

Показано [4], что мы можем сформулировать методику выбора оптимального множества значений качественных признаков. Более того, показано, что такая методика является устойчивой, то есть возможные при построении функций принадлежности естественные маленькие ошибки не оказывают существенного влияния на выбор оптимального множества значений. Множества, оптимальные по критериям 1 и 2 совпадают.

Проблема 2. Можно ли определить показатели качества поиска информации в нечетких (лингвистических) базах данных и сформулировать правило выбора такого множества лингвистических значений, использование которого обеспечивало бы максимальные показатели качества поиска информации?

Показано [2], что можно ввести показатели качества поиска информации в нечетких (лингвистических) базах данных и формализовать их. Показано, что возможно сформулировать методику выбора оптимального множества значений качественных признаков, которое обеспечивает максимальные показатели качества поиска информации. Более того, показано, что такая методика является устойчивой, то есть возможные при построении функций принадлежности естественные маленькие ошибки не оказывают существенного влияния на выбор оптимального множества значений.

Проблема 3. Можно ли предложить процедуры выбора операторов агрегирования информации в нечетких иерархических динамических системах, минимизирующих противоречивость модели проблемы/процесса в системах информационного мониторинга?

Можно выделить следующие подходы к решению этой проблемы, базирующиеся на различных интерпретациях операторов агрегирования информации [3]: геометрический, логический и подход на основе обучения, включающий в себя обучение на основе генетических алгоритмов и обучение на основе нейронных сетей.

Список литературы

1. Рыжов А. П. Информационный мониторинг сложных процессов: технологические и математические основы // Интеллектуальные системы. — Т. 11, вып. 1–4. — С. 101–136.

2. Рыжов А. П. Модели поиска информации в нечеткой среде. — М.: Изд-во ЦПИ при мех-мат ф-те МГУ, 2004.

3. Рыжов А. П. Об агрегировании информации в нечетких иерархических системах // Интеллектуальные системы. — 2001. — Т. 6, вып. 1–4. — С. 341.

4. Рыжов А. П. Элементы теории нечетких множеств и измерения нечеткости. — М.: Диалог-МГУ, 1998.

ГОМОМОРФИЗМЫ ИГР С ОТНОШЕНИЯМИ ПРЕДПОЧТЕНИЯ

Т. Ф. Савина (Саратов)

Математическая теория игр занимается построением и исследованием математических моделей принятия решений в условиях конфликта, который возникает за счет различия интересов принимающих решение систем. В классической теории игр интересы игроков задаются при помощи целевых функций. Однако на практике построение таких функций сопряжено со значительными трудностями. В настоящей работе рассматривается класс игр, в которых цели игроков формализуются в виде бинарных отношений на множестве исходов.

Игра n ($n \geq 2$) игроков с отношениями предпочтения определяется как система объектов

$$G = \langle X_1, \ldots, X_n, A, \rho_1, \ldots, \rho_n, F \rangle,$$

где X_i — множество стратегий игрока i ($i = 1, \ldots, n$), A — множество исходов, F — отображение множества ситуаций $X_1 \times \ldots \times X_n$ в множество исходов A, ρ_i — отношение предпочтения игрока i ($i = 1, \ldots, n$), заданное на A.

Основной задачей теории игр является нахождение оптимальных решений, при этом известны теоретические результаты об оптимальных решениях игр с отношениями предпочтения специального вида (например, с отношениями порядка [1]). Так как на практике отношения предпочтения задаются при помощи графов, то соответствующие математические модели бывают весьма громоздкими. Основной метод их упрощения состоит в переходе от игры к ее гомоморфному образу.

Для произвольной игры с отношениями предпочтения мы можем построить подобную ей игру более простого вида — фактор-игру. В данной статье исследуется вопрос о том, когда фактор-игра будет игрой с отношениями предпочтения специального вида. В частности, решены задачи — когда фактор-игра будет игрой с транзитивной структурой предпочтений [2] и игрой с ациклической структурой предпочтений. Решение дается в виде условий, накладываемых на систему эквивалентностей, по которым производится факторизация, причем эти условия записываются в виде элементарных формул на языке теории бинарных отношений.

Пусть теперь, кроме игры G, задана еще одна игра с отношениями предпочтения тех же игроков $\Gamma = \langle U_1, \ldots, U_n, B, \sigma_1, \ldots, \sigma_n, \Phi \rangle$.

Определение 1. Набор отображений $\varphi = (\varphi_1, \ldots, \varphi_n, \varphi_{n+1})$, где $\varphi_i \colon X_i \to U_i$ $(i = 1, \ldots, n)$, $\varphi_{n+1} \colon A \to B$ называется *гомоморфизмом игры G в игру* Γ, если выполняются следующие условия:

$$a_1 \overset{\rho_i}{\lesssim} a_2 \;\Rightarrow\; \varphi_{n+1}(a_1) \overset{\sigma_i}{\lesssim} \varphi_{n+1}(a_2) \quad (i = 1, \ldots, n), \qquad (H1)$$

$$\varphi_{n+1} \circ F = \Phi \circ (\varphi_1 \square \ldots \square \varphi_n).$$

Гомоморфизм φ игры G в игру Γ называется *строгим*, если условие $(H1)$ заменяется более сильной системой условий:

$$a_1 \overset{\rho_i}{<} a_2 \;\Rightarrow\; \varphi_{n+1}(a_1) \overset{\sigma_i}{<} \varphi_{n+1}(a_2) \quad (i = 1, \ldots, n),$$

$$a_1 \overset{\rho_i}{\sim} a_2 \;\Rightarrow\; \varphi_{n+1}(a_1) \overset{\sigma_i}{\sim} \varphi_{n+1}(a_2) \quad (i = 1, \ldots, n).$$

Определение 2. Набор эквивалентностей $\varepsilon = (\varepsilon_1, \ldots, \varepsilon_n, \varepsilon_{n+1})$, где $\varepsilon_i \subseteq X_i^2$ $(i = 1, \ldots, n)$, $\varepsilon_{n+1} \subseteq A^2$, называется *конгруэнтностью в игре G*, если для этого набора выполняется условие согласованности для функции реализации, которое имеет вид:

$$\left.\begin{array}{ll} x_1' & \overset{\varepsilon_1}{\equiv} \; x_1 \\ x_2' & \overset{\varepsilon_2}{\equiv} \; x_2 \\ & \ldots \\ x_n' & \overset{\varepsilon_n}{\equiv} \; x_n \end{array}\right\} \Rightarrow F(x_1', \ldots, x_n') \overset{\varepsilon_{n+1}}{\equiv} F(x_1, \ldots, x_n).$$

Конгруэнтность ε в игре G называется *str-конгруэнтностью*, если выполняется дополнительное условие согласованности для отношений предпочтения:

$$a_1 \overset{\rho}{\lesssim} a_2 \wedge a_1' \overset{\varepsilon}{\equiv} a_1 \wedge a_2' \overset{\varepsilon}{\equiv} a_2 \wedge a_2' \overset{\rho}{\lesssim} a_1' \Rightarrow a_1 \overset{\rho}{\sim} a_2.$$

Теорема 1. *Пусть G — игра с отношениями предпочтения, на которой задана конгруэнтность ε. Тогда определена фактор-игра*

$$G/\varepsilon = \langle X_1/\varepsilon_1, \ldots, X_n/\varepsilon_n,\ A/\varepsilon_{n+1},\ \rho_1/\varepsilon_{n+1}, \ldots, \rho_n/\varepsilon_{n+1},\ F_{\varepsilon_{n+1}} \rangle$$

с отношениями предпочтения и каноническое отображение $\varphi_\varepsilon = (\varphi_{\varepsilon_1}, \ldots, \varphi_{\varepsilon_n}, \varphi_{\varepsilon_{n+1}})$, где $\varphi_{\varepsilon_i} \colon X_i \to X_i/\varepsilon_i$ $(i = 1, \ldots, n)$, $\varphi_{\varepsilon_{n+1}} \colon A \to A/\varepsilon_{n+1}$ и $F_{\varepsilon_{n+1}}([x_1]_{\varepsilon_1}, \ldots, [x_n]_{\varepsilon_n}) \overset{df}{=} [F(x_1, \ldots, x_n)]_{\varepsilon_{n+1}}$, будет сюръективным гомоморфизмом игры G на G/ε.

При этом, если конгруэнтность ε является str-конгруэнтностью, то каноническое отображение φ_ε будет строгим гомоморфизмом.

Теорема 2. *Пусть G — игра с отношениями предпочтения, на которой задана конгруэнтность ε. Для того, чтобы факторигра G/ε была игрой с транзитивной структурой предпочтений необходимо и достаточно, чтобы выполнялось условие:*

$$\rho_i \circ \varepsilon_{n+1} \circ \rho_i \subseteq \varepsilon_{n+1} \circ \rho_i \circ \varepsilon_{n+1} \quad (i = 1, \ldots, n).$$

Теорема 3. *Пусть G — игра с отношениями предпочтения, на которой задана конгруэнтность ε. Для того, чтобы фактор-игра G/ε была игрой с ациклической структурой предпочтений необходимо и достаточно, чтобы для всех $i = 1, \ldots, n$ отношение $\rho_i \cup \varepsilon_{n+1}$ было ациклическим относительно ε_{n+1}, т. е. выполнялась импликация:*

$$a_0 \overset{\rho_i \cup \varepsilon_{n+1}}{\lesssim} a_1 \overset{\rho_i \cup \varepsilon_{n+1}}{\lesssim} \ldots \overset{\rho_i \cup \varepsilon_{n+1}}{\lesssim} a_n \overset{\rho_i \cup \varepsilon_{n+1}}{\lesssim} a_0 \Rightarrow a_0 \overset{\varepsilon_{n+1}}{\equiv} a_1 \overset{\varepsilon_{n+1}}{\equiv} \ldots \overset{\varepsilon_{n+1}}{\equiv} a_n$$

Список литературы

1. Розен В. В. Гомоморфизмы игр с упорядоченными исходами // Математические модели поведения. Методы и модели принятия решений. Межвуз. науч. сб. — Саратов: Изд-во СГУ, 1981. — С. 90–104.

2. Савина Т. Ф. Гомоморфизмы и конгруэнтности игр с транзитивной структурой предпочтений // Материалы Междунар. науч. конф. "Компьютерные науки и информационные технологии" (1–4 июля 2009 г.). — Саратов: Изд-во СГУ, 2009. — С. 157–160.

О СВОЙСТВАХ ГИПЕРАВТОМАТОВ

И. Ю. Самоненко (Москва)

Обозначим $E_k = \{0, \ldots, k-1\}$. Пусть X — конечное множество, n и s — натуральные числа. Через $< x_1, ..., x_n >$ обозначим мультимножество состоящее из элементов $x_1, \ldots, x_n$, т. е. $< x_1, ..., x_n >= \{(x_{i_1}, t_{i_1}), \ldots, (x_{i_s}, t_{i_s})\}$, где число вхождений элемента x_{i_j} в вектор $(x_1, ..., x_n)$ равно t_{i_j}, $j = 1, \ldots, s$ и $t_{i_1} + \cdots + t_{i_s} = n$. Обозначим

$$p_1(x_1, \ldots, x_s) = (x_1, \ldots, x_s),$$
$$p_2(x_1, \ldots, x_s) =< x_1, \ldots, x_s >,$$
$$p_3(x_1, \ldots, x_s) = \{x_1, \ldots, x_s\}.$$

Определим $X^{(s,i)} = \{p_i(x_1, \ldots, x_s) | x_i \in X\}$, $i = 1, 2, 3$.

Пусть $\mathbf{A} = (A, Q, \varphi)$ — конечный автомат. Автомат $\mathbf{B}_i = \mathbf{A}^{(s,i)} = (A, Q^{(s,i)}, \varphi^{(s,i)})$ называется s-гипераавтоматом i-ого типа ($i = 1, 2, 3$) порожденным автоматом $\mathbf{A}$, где

$$\varphi^{(s,i)}(p_i(q_1, \ldots, q_s), a) = p_i(\varphi(q_1, a), \ldots, \varphi(q_s, a)).$$

Автомат $\mathbf{A}$ назовем базой гипераавтомата $\mathbf{A}^{(s,i)}$. Базовым числом состояний гипераавтомата $\mathbf{A}^{(s,i)}$ назовем число состояний автомата $\mathbf{A}$.

Пусть $\mathbf{A} = (A, Q, \varphi)$ — конечный автомат, $q_0 \in Q$ и $F \subseteq Q$, тогда через $L(\mathbf{A}, q_0, F)$ обозначим регулярный язык представимый в автомате $\mathbf{A}$ при помощи начального состояния q_0 и множества финальных состояний F. Через $L(\mathbf{A}) = \{L(\mathbf{A}, q_0, F) | q_0 \in Q,\ F \subseteq Q\}$ обозначим множество всех регулярных языков, представимых в автомате $\mathbf{A}$.

Пусть Ω — некоторое множество автоматов. Для произвольного множества автоматов Ω обозначим $\Omega^{(s,i)} = \cup_{\mathbf{A} \in \Omega} \mathbf{A}^{(s,i)}$. Через $L(\Omega) = \cup_{\mathbf{A} \in \Omega} L(\mathbf{A})$ обозначим множество всех регулярных языков представимых автоматами из множества Ω. Через $N(\Omega) = max_{\mathbf{A} \in \Omega}(|L(\mathbf{A})|)$ обозначим максимальное число языков представимое в некотором автомате $\mathbf{A} \in \Omega$. Обозначим $N_i(\Omega, s) = N(\Omega^{(s,i)})$, $i = 1, 2, 3$.

Через Ω_n обозначим множество всех автоматов с n состояниями и $|A| \geq 3$. Через Ω'_n обозначим множество всех групповых автоматов с n состояниями и $|A| \geq 2$. Обозначим $N_i(n, s) = N_i(\Omega_n, s)$ и $N'_i(n, s) = N_i(\Omega'_n, s)$. Обозначим $U(n, s, x) = \frac{n!}{s!(n-s)!} 2^x$.

Теорема. *При фиксированном s и $n \to \infty$ справедливы следующие утверждения:*

1. $N_1(n, s) \sim U(n, s, n^s)$, $N'_1(n, s) \sim U(n, s, \frac{n!}{(n-s)!})$.
2. $N_2(n, s) \sim U(n, s, \frac{(n+s-1)!}{s!(n-1)!})$, $N'_2(n, s) \sim U(n, s, \frac{n!}{s!(n-s)!})$.
3. $N_3(n, s) \sim U(n, s, \sum_{t=1}^{s} \frac{n!}{t!(n-t)!})$, $N'_3(n, s) \sim U(n, s, \frac{n!}{s!(n-s)!})$.

Список литературы

1. Кудрявцев В. Б., Алёшин С. В., Подколзин А. С. Введение в теорию автоматов. — М., 1985.

2. Самоненко И. Ю. Об r-предсказуемости автоматных сетей // Интеллектуальные системы. — 2007. — Т. 11. — С. 787.

СРАВНИТЕЛЬНЫЙ АНАЛИЗ АЛГОРИТМОВ ЦЕЛОЧИСЛЕННОГО СБАЛАНСИРОВАНИЯ МАТРИЦЫ

А. В. Смирнов (Ярославль)

В [1] дана постановка задачи целочисленного сбалансирования трехмерной матрицы. Имеется трехмерная вещественная матрица A с неотрицательными элементами a_{ijp} ($i \in \overline{0,n},\ j \in \overline{0,m},\ p \in \overline{0,t}$), для которых выполнены условия баланса: каждый элемент с некоторыми нулевыми индексами равен сумме всех элементов, для которых ненулевые индексы оставлены неизменными, а нулевые индексы заменены всеми возможными ненулевыми значениями диапазонов соответствующих индексов.

Требуется так округлить элементы матрицы до целых значений сверху или снизу (элемент a_{000} округляется до ближайшего целого), чтобы остались неизменными условия баланса.

Для решения поставленной задачи в [1] предложено обобщение теории потоков Форда—Фалкерсона, названное кратными потоками и задачей о нахождении максимального кратного потока. Там же приводится схема сведения задачи сбалансирования к потоковой. При этом решению задачи сбалансирования соответствует некоторый максимальный поток величины $[a_{000} + 0.5]$. Если же максимальный поток в кратной сети целочисленного сбалансирования оказывается меньше, чем $[a_{000} + 0.5]$, то задача сбалансирования не имеет решения.

Как и в алгоритме Форда—Фалкерсона, получение максимального кратного потока может быть разделено на два этапа: получение полного потока и, если полный поток не является максимальным, то увеличение потока при помощи обобщенного алгоритма пометок, пока не будет получен максимальный поток. В связи с тем, что максимальный поток не всегда индуцирует решение задачи, вводится дополнительный этап коррекции потока, на котором используется некоторая модификация обобщенного алгоритма пометок.

Идея обобщенного алгоритма пометок состоит в следующем: в *проекциях* G_1 *и* G_2 (определение см. в [1]) поочередно строится путь прорыва (возможно, в объединении с некоторыми циклами) до тех пор, пока пути в обеих проекциях не станут *согласованными*, либо же не останется вариантов для продолжения построения пути. В первом случае объединение путей прорыва в частях G_1 и G_2 с мультидугой с концом в z даст *обобщенный путь прорыва* [1], во втором случае производится откат до так называемой "точки ветвления", после чего выполнение алгоритма возобновляется. Если точкой ветвления оказывается x_{000}, то задача целочисленного сбалансирования не имеет решения.

Теорема. *Если решение задачи целочисленного сбалансирования существует, то оно может быть найдено при помощи обобщенного алгоритма пометок.*

Задача целочисленного сбалансирования может быть сведена также к задаче целочисленного линейного программирования. Такое сведение было рассмотрено в [2]. В этом случае решение задачи сбалансирование может быть найдено при помощи первого алгоритма Гомори (определение см. в [3]).

Сравним два алгоритма. При этом заметим, что оба алгоритма имеют экспоненциальную трудоемкость. Обратимся к результатам вычислительных экспериментов.

Результаты экспериментов показали, что алгоритм Гомори, как правило, оказывается предпочтительней в случае, когда задача целочисленного сбалансирования не имеет решений. Действительно, в этом случае в обобщенном алгоритме пометок неизбежно возникает полный перебор всех вариантов. Также предпочтительней оказывается метод Гомори в случаях, когда количество переменных и количество целочисленных суммирующих показателей в исходной матрице близки, либо же целых сумм больше, чем переменных.

В случае же, когда в исходной матрице нет целых сумм, или же их количество относительно мало, более эффективным на большинстве тестов (в 87,8 % случаев в среднем по таким примерам) оказывается обобщенный алгоритм пометок. Тем не менее полный перебор может возникнуть и в этих ситуациях.

Отметим также, что в тех случаях, когда обобщенный алгоритм пометок оказывался быстрее метода Гомори, время выполнения алгоритмов отличалось в среднем на порядок.

Исходя из вышесказанного, можно предложить следующую схему действий:

1) необходимо установить максимальное допустимое время выполнения алгоритма, зависящее от размерности матрицы и производительности компьютера;

2) необходимо определить, какой из алгоритмов будет запущен первым. В случае наличия большого числа целых сумм целесообразно выбрать метод Гомори, в противном случае – алгоритм пометок;

3) выполняем выбранный алгоритм до тех пор, пока не будет получен ответ, либо не будет превышено максимальное допустимое время;

4) если было превышено допустимое время, то выполняем шаг 3 для второго алгоритма; если время опять превышается, выдаем ошибку.

Гипотеза. *Задача целочисленного сбалансирования трехмерной матрицы является NP-трудной.*

Список литературы

1. Рублев В. С., Смирнов А. В. Целочисленное сбалансирование 3-мерной матрицы плана // Труды VII международной конференции "Дискретные модели в теории управляющих систем" (Покровское, 4–6 марта 2006 г.). — М.: Изд-во ф-та ВМК МГУ, 2006. — С. 302–308.

2. Смирнов А. В. Задача целочисленного сбалансирования трехмерной матрицы и сетевая модель // Моделирование и анализ информационных систем. — 2009. — Т. 16, 3. — С. 70–76.

3. Корбут А. А., Финкельштейн Ю. Ю. Дискретное программирование — М.: Наука, 1969.

КРИТЕРИЙ СВОДИМОСТИ ЗАДАЧИ ОБ ОПАСНОЙ БЛИЗОСТИ К ЗАДАЧЕ ОДНОМЕРНОГО ИНТЕРВАЛЬНОГО ПОИСКА

Е. А. Снегова (Москва)

В работе исследуется задача о поиске движущихся объектов, которые могут столкнуться с движущимся объектом-запросом, где под столкновением понимается нахождение объектов в опасной близости.

Пусть заданы две функции $f : [0, \tau_{max}] \to [-\rho, 1+\rho]$ и $f_q : [0, \tau^q_{max}] \to [-\rho, 1+\rho]$, называемые законами движения объектов и объектов-запросов, соответственно. Считаем, что имеется счетное множество объектов, движущихся на плоскости таким образом, что их координаты в зависимости от времени задаются парой $(f(t-t_i), y_i)$, где $i \in N$, $y_i \in [0,1]$, а t_i образует строго возрастающую последовательность положительных чисел. Аналогично, движение объекта-запроса задается парой $(x, f_q(t-t_q))$, где $x \in [0,1]$, $t_q \geq 0$.

Множество $V(t_q) = \{(t_i, y_i) : (f(t_q - t_i), y_i) \in [-\rho, 1+\rho] \times [0,1]\}$ назовем библиотекой в момент t_q. Вместо $V(t_q)$ будем писать просто V, понимая под этим множество всех объектов, находящихся в текущий момент времени внутри квадрата. Через $|V|$ обозначим число объектов в библиотеке.

В задаче требуется для произвольного запроса перечислить все объекты из библиотеки, с которыми он в процессе своего движения будет находиться на расстоянии меньшем, чем ρ по Манхэттену.

Ответ на запрос $q = (t_q, x)$ при библиотеке V и расстоянии опасной близости ρ обозначим как $J(\rho, q, V)$.

Тройку (f, f_q, ρ) будем называть *задачей об опасной близости.*

Основной характеристикой алгоритма решения этой задачи является сложность поиска, измеряемая в операциях вычисления значений некоторых функций, принятых за элементарные. Поскольку библиотека динамически меняется со временем, то важными характеристиками являются также сложности вставки и удаления объектов в БД. Еще одной характеристикой является объем памяти, требуемый алгоритму для хранения структур данных.

Задачей одномерного интервального поиска назовем пару (I, Z), где библиотека Z — конечное подмножество $[0, 1]$, а множество запросов I — есть множество всех интервалов, содержащихся в $[0, 1]$. Содержательно эта задача состоит в том, чтобы для произвольного запроса $p \in I$ перечислить все те и только те точки из Z, которые попадают в интервал p.

Ответ на запрос $p \in I$ при библиотеке Z в задаче одномерного интервального поиска есть множество $J(p, Z) = \{z \in Z : z \in p\}$.

Будем говорить, что задача об опасной близости (f, f_q, ρ) *сводится* с задаче одномерного интервального поиска, если существуют такие отображения $\varphi, \varphi_1, \varphi_2 : R \times [0, 1] \to [0, 1]$, что для любой библиотеки V, любого запроса q и любого объекта $o \in V$ верно $o \in J(\rho, q, V) \Leftrightarrow \varphi(o) \in J([\varphi_1(q), \varphi_2(q)], Z)$, где $Z = \{\varphi(o) : o \in V\}$.

В [1] рассматривался случай фиксированных скоростей объектов, то есть $f(t) = vt$, а $f_q(t) = v_q t$, в [2] рассматривался случай, когда $f'(t + t') - f'_q(t) \leq 0$ для любого $t \in [0, \tau^q_{max}]$ и любого t', такого, что $t + t' \in [0, \tau_{max}]$. В обоих случаях задача решалась путем сведения задачи об опасной близости к задаче одномерного интервального поиска, которая имеет логарифмическую относительного общего числа объектов в библиотеке сложность поиска вставки и удаления, и линейный объем памяти.

Обозначим:

$$F_L(x, y) = \min_{\xi \in [0, \rho]} [f_q^{-1}(y + \xi - \rho) - f^{-1}(x + \xi)],$$

$$F_R(x, y) = \max_{\xi \in [-\rho, 0]} [f_q^{-1}(y + \xi + \rho) - f^{-1}(x + \xi)].$$

Теорема. *Задача об опасной близости (f, f_q, ρ) сводится к задаче одномерного интервального поиска тогда и только тогда, когда существуют функции $\psi, \psi_L, \psi_R : [0, 1] \to R$ такие, что:*

$$F_L(x, y) = \psi(y) + \psi_L(x) \ \ \forall (x, y) : F_L(x, y) \leq 0, \tag{1}$$

$$F_R(x,y) = \psi(y) + \psi_R(x) \;\; \forall (x,y) : F_R(x,y) \le 0. \qquad (2)$$

Следствие. *Пусть для тройки* (f, f_q, ρ) *существуют функции* $\psi, \psi_L, \psi_R : [0,1] \to R$ *такие, что для них выполнено* (1) *и* (2). *Тогда существует алгоритм* A *решающий задачу об опасной близости* (f, f_q, ρ). *Для сложности поиска ответа на любой запрос* q, *вставки любого объекта-данного* o, *удаления любого объекта-данного* $\tilde{o}$ *по алгоритму* A, *и для объема алгоритма* A *верны следующие оценки:*

$$T_A(\rho, q, V) = O(\log_2 |V|),$$

$$S_A(\rho, o, V) = O(\log_2 |V|),$$

$$R_A(\rho, \tilde{o}, V) = O(\log_2 |V|),$$

$$Q_A(\rho, V) = O(|V|),$$

где за элементарные операции приняты операции сложения и сравнения чисел, а также операции вычисления значения любой из функций ψ, ψ_L, ψ_R *в любой точке из отрезка* $[0,1]$.

Работа выполнена на кафедре МаТИС механико-математического факультета МГУ. Научный руководитель — профессор Гасанов Э. Э.

Список литературы

1. Скиба Е. А. Логарифмическое решение задачи об опасной близости // Интеллектуальные системы. — 2007. — Т. 11, вып. 1–4.

2. Снегова Е. А. Случай задачи об опасной близости, сводящийся к одномерному интервальному поиску // Интеллектуальные системы. — В печати.

ОБ ОДНОМ СЕМЕЙСТВЕ НЕЙРОНОВ С ОГРАНИЧЕННОЙ СЛОЖНОСТЬЮ ВЗАИМНОЙ ПЕРЕСТРОЙКИ

А. П. Соколов (Москва)

Пороговые функции алгебры логики являются математической моделью нейронов. Они представляют интерес благодаря своим универсальным вычислительным возможностям, а также благодаря возможности их обучения. Последнее свойство с успехом применяется на практике при решении плохоформализуемых задач.

В качестве средства задания пороговых функций в работе рассматриваются линейные формы вида $x_1 w_1 + ... + x_n w_n - \sigma$ с целочисленными коэффициентами и свободным членом.

Исследуется сложность преобразования одной пороговой функции, заданной линейной формой, к другой, путем пошагового изменения коэффициентов линейной формы. В качестве меры сложности данного процесса принимается изменение коэффициента или свободного члена линейной формы на единицу. Данный процесс может интерпретироваться как процесс обучения нейрона с пороговой функцией активации.

Ранее, в работе [1], для характеризации сложности обучения в худшем случае исследовалась шенноновская функция $\rho(n)$. Она говорит о том, сколько минимально достаточно выполнить единичных модификаций исходной линейной формы от n переменных для задания желаемой пороговой функции. Было показано, что при стремлении n к бесконечности величина $\log_2 \rho(n)$ растет по порядку как $n \log_2 n$.

Естественным образом возникает вопрос о том, как ведет себя расстояние между пороговыми функциями в большинстве случаев.

В работе [2] был построен пример такого класса пороговых фукнций, что для почти всех функций из данного класса расстояние между ними "велико" (зависит экспоненциально от числа переменных). При этом, мощность данного класса в некотором смысле сопоставима с мощностью класса всех пороговых функций.

В настоящей работе приводится конструктивное построение такого класса пороговых фукнций, что расстояние между функциями из данного класса ограничено заранее заданной величиной, лежащей в диапазоне от $3 \cdot n$ до $3 \cdot 2^n$, где n — число переменных. При этом, мощность данного класса экспоненциально зависит от n.

Пусть $U = \{u_1, u_2, ...\}$ — счетный алфавит переменных. Каждое из переменных u_i может принимать значения из множества $E_2 = \{0, 1\}$. В дальнейшем во избежание употребления сложных индексов мы будем использовать для обозначения букв алфавита U метасимволы x_i с индексами или без них.

Введем определения линейной формы и пороговой функции.

Линейной формой назовем функцию вида

$$l_{\vec{w},\sigma}(x_1, ..., x_n) = \sum_{i=1}^{n} x_i w_i - \sigma,$$

где w_i и σ суть целые числа при $i = 1, ..., n$.

Вектор $\vec{w} = (w_1, ..., w_n)$ называют вектором весовых коэффициентов, а σ — порогом.

Функция $f(x_1, ..., x_n) : E_2^n \to E_2$, называется *пороговой*, если существует линейная форма $l_{\vec{w},\sigma}(x_1, ..., x_n) = x_1 w_1 + ... + x_n w_n - \sigma$ такая, что

$$f(x_1, ..., x_n) = \begin{cases} 1, \textit{ если } \sum\limits_{i=1}^{n} x_i w_i - \sigma \geq 0; \\ 0, \textit{ иначе.} \end{cases}$$

В этом случае говорим, что *линейная форма* $l_{\vec{w},\sigma}$ *задает пороговую функцию* $f(x_1, ..., x_n)$, и записывается это так:

$$l_{\vec{w},\sigma} \to f(x_1, ..., x_n),$$

или просто $f_{\vec{w},\sigma}$.

Множество всех пороговых функций от n переменных $x_1, ..., x_n$ обозначим T^n.

В связи с тем, что линейные формы с целочисленными коэффициентами и порогом позволяют задать любую пороговую функцию, далее в работе рассматриваются только такие линейные формы.

Введем понятие расстояния между линейными формами и пороговыми функциями.

Пусть $l_{\vec{w}',\sigma'}$ и $l_{\vec{w}'',\sigma''}$ — линейные формы от n переменных. Расстоянием между линейными формами $l_{\vec{w}',\sigma'}$ и $l_{\vec{w}'',\sigma''}$ назовем следующую величину

$$\rho(l_{\vec{w}',\sigma'}; l_{\vec{w}'',\sigma''}) = |\sigma' - \sigma''| + \sum_{i=1}^{n} |w_i' - w_i''|.$$

Эту величину интерпретируем как необходимость сделать ρ последовательных единичных изменений компонент одной линейной формы, чтобы получить другую.

Расстоянием между пороговыми функциями $f'(x_1, ..., x_n)$ и $f''(x_1, ..., x_n)$ назовем величину

$$\rho(f'; f'') = \min_{\substack{l_{\vec{w}',\sigma'} \to f' \\ l_{\vec{w}'',\sigma''} \to f''}} \rho(l'; l'').$$

Здесь минимум берется по всем линейным формам $l_{\vec{w}',\sigma'}$ и $l_{\vec{w}'',\sigma''}$, задающим функции f' и f'', соответственно.

Сформулируем основной результат работы.

Теорема. *Если* $n + 1 \leq c \leq 2^{\frac{n}{2}}$, *то существует класс* M *пороговых функций от* n *переменных, содержащий* $(c - n - 1) \cdot 2^{n-2}$ *элементов, такой что для всех* f', f'' *из* M *выполнено*

$$\rho(f', f'') \leq 3 \cdot c.$$

Список литературы

1. Кострикин А. И. Введение в алгебру. Линейная алгебра. — М.: Физматлит, 2000.

2. Соколов А. П. О конструктивной характеризации пороговых функций // Интеллектуальные системы. — 2008. — Т. 12, вып. 1–4. — С. 363–388.

2. Соколов А. П. О сложности обучения в одном классе нейронов // Интеллектуальные системы. — 2009. — Т. 13, вып. 1–4.

ОБ АЛГОРИТМИЧЕСКИХ ВОПРОСАХ МОДЕЛИРОВАНИЯ ПРОЦЕССА ОБУЧЕНИЯ

А. С. Строгалов (Москва)

Основной проблемой при использовании компьютеров в обучении и образовании является создание не только уникальных с точки зрения возможностей обучения систем, но также и создание технологий их разработки, поддержки, обновления содержания и пр., включая вопросы тиражирования и распространения.

Одним из главных остается так же вопрос о том как делать компьютерные обучающие системы, обладающих как развитыми техническими возможностями по обработке учебной информации, так и нетривиальными и интеллектуальными функциями преподавателя? Ответ на этот вопрос, несмотря на явный рост технических возможностей компьютеров по представлению, отображению и обработке информации, находится в исследовательской стадии, хотя есть и многочисленные обнадеживающие результаты [1–6], полученные нами в процессе создания реальных компьютерных систем обучения.

Примером решения проблем создания технологического инструментария для разработки интеллектуальных обучающих систем является проект "IDEA" (создание экспертных систем в области обучения в различных предметных областях) [7]. В нем предлагалось создание на основе автоматных моделей строить модели ученика и учителя, которые взаимодействуют между собой через пространство учебного материала, формализованного в виде,например, размеченных информационных деревьев или нагруженных графов более общего вида. Удалось построить удачные примеры версий обучающих систем в области изучения иностранных языков (в том числе

и с применением экспертной системы), которые однако не были развиты до своего полного завершения из-за необходимости создания большого набора решающих правил, что требовало больших затрат ресурсов, которыми организаторы работ в то время не обладали.

На основе инструментальной среды "IDEA Professional" был создан ряд мультимедийных обучающих и тестирующих систем, электронных монографий по информатике, гуманитарным наукам, медицине и другим предметным областям. Отрабатывался опыт эффективного использования телекоммуникаций в обучении в режимах "off-line" и "on-line". Всего за 1995–2008 гг. было произведено порядка 20 курсов, часть из которых была доведена до тиража и выпущена на отечественный рынок образовательных услуг.

Опишем некоторую формализацию процесса обучения, лежащую в основе проекта "IDEA", которая может быть уточнена до математической модели в виде автоматной схемы [6].

Учебный материал представляется в виде набора деревьев, имеющих перекрестные ссылки, что отражает не только иерархичность структуры обучающего материала, но и различного рода ссылки, создающие вторичные и пр. структуры учебного материала, отражающие взаимосвязи различных учебных целей, задач и т. д. В зависимости от типа ученика , его успехов или неудач предлагалось три стратегии обучения (быстрая, нормальная и медленная). Экспертная система имела набор правил продукционного типа (*Если* <условие> *то* <действие>) с разработанными редактором и компилятором для системы продукций. Для экспертной системы был разработан специальный механизм оценки качества событий, происходящих с ее участием (например, локальная оценка качества учебного процесса на основе выбранной стратегии) в виде достаточно большого набора кривых, допускающих естественную интерпретацию типа "прогресс", "единичная ошибка", "нарастание усталости" и т. д.

В этом подходе учитель и ученик интерпретировались как адаптивные автоматы, а процесс обучения состоял их итеративном взаимодействии. Со стороны автомата-учителя на каждом шаге выбирается оптимальная с его точки зрения подача автомату-ученику обучающей информации на основе того, как "усвоил" на предыдущих шагах обучения такую информацию автомат- ученик.

В соответствии со сказанным в проблеме синтеза адаптивного компьютерного "учителя" необходимо было решение следующих основных задач: 1) синтез автомата-учителя; 2) синтез автомата-ученика; 3) разработка информационной системы, аналогичной учебнику с упражнениями; 4) выработка оптимальной стратегии взаимодействия компонент 1–4; 5) создание интерфейса с широкими сервисными услугами для пользователя.

Решение задач 1–4 сопряжено с рассмотрением целого ряда вопросов. К их числу относятся: а) разработка динамических баз данных и знаний, состоящих из больших массивов синтаксической информации со сложной семантикой и нечеткими логическими связями; б) разработка признакового пространства описания состояний автоматов-учителя и -ученика с указанием функционально-метрических зависимостей между ними, позволяющими задавать функционирование этих автоматов; в) разработка оптимальных стратегий взаимодействия автомата-учителя с автоматом-учеником как средствами собственно теории автоматов и нечеткой логики, так и процедурами типа распознавания образов и пр.

Таким образом, учебный курс, содержащий достаточное количество стратегий, позволяет экспертной системе подойти к ученику индивидуально. Разумеется, в процессе обучения могут возникнуть локальные отклонения от стратегии, связанные с решениями экспертной системы или самого ученика, но глобальная задача экспертной системы — провести ученика по выбранной стратегии и, следовательно, решить соответствующую этой стратегии задачу обучения — достигается.

Список литературы

1. Кудрявцев В. Б., Вашик К., Строгалов А. С., Алисейчик П. А., Перетрухин В. В. Об автоматном моделировании процесса обучения // Дискретная математика. — 1996. — Т. 8, вып. 4. — С. 3–10.

2. Подколзин А. С. О формализации приемов решения математических задач // Интеллектуальные системы. — 1998. — Т. 3, вып. 3–4. — С. 51–74.

3. Строгалов А. С., Шеховцов С. Г. Мышление, язык и интеллектуальное образование // Интеллектуальные системы. — 1998. — Т. 3, вып. 3–4. — С. 5–50.

4. Афанасьев Ю. Н., Строгалов А. С., Шеховцов С. Г. Об универсальном знании и новой образовательной среде (к концепции универсальной компоненты образования). — М.: Изд-во РГГУ, 1999.

5. Строгалов А. С. Существует ли гуманитарный аспект математики? // Математика и общество. Математическое образование на рубеже веков. Сборник. — М.: Изд-во МНЦМО, 2000.

6. Алисейчик П. А., Вашик К., Кудрявцев В. Б., Строгалов А. С., Шеховцов С. Г. Компьютерные обучающие системы // Интеллектуальные системы. — 2007. Т. 10, вып. 1–4. — С. 189–270.

7. Вашик К., Кудрявцев В. Б., Строгалов А. С. Проект IDEA. Введение в новое поколение программного обеспечения типа ICBI для передачи знаний и навыков с помощью экспертной системы. — Link @ Link Software GmbH, Dortmund, Germany, 1995.

ОБЩИЙ ПОДХОД К ВОССТАНОВЛЕНИЮ ГРАФОВ ПРИ ПОМОЩИ БЛУЖДАЮЩЕГО ПО НИМ АГЕНТА

Е. А. Татаринов (Донецк)

Рассматривается задача восстановления конечного, неориентированного, связного графа G, без петель и кратных ребер, при помощи агента (робота, конечного автомата) [1]. Задан агент, который может передвигаться из вершины в вершину неизвестного ему графа G по ребру, соединяющему их, воспринимать и анализировать некоторую локальную информацию об 1 — окрестности вершины, в которой он находится. Агент обладает набором средств для изменения меток элементов графа, конечной, но бесконечно наращиваемой памятью, в которой он будет строить граф H изоморфный графу G, с точностью до меток на элементах графов. Изначально предполагается, что элементы графа G не помечены, а агент помещается в произвольную его вершину.

Требуется построить такой метод обхода вершин, ребер графа G и разметки его элементов, что бы можно было построить граф H изоморфный графу G с точностью до меток на элементах графов.

Известен ряд алгоритмов, решающих задачу восстановления графа принадлежащего некоторому классу [2, 3]. Агенты, реализующие эксперимент по восстановлению графа, обладали различными сенсорными возможностями, ресурсами для раскраски элементов графа, памятью и априорными знаниями о свойствах восстанавливаемого графа. Анализ существующих алгоритмов решения задачи восстановления графа позволил выделить общий подход. Суть подхода в следующем: перенумеровать (явно или неявно) вершины восстанавливаемого графа G номерами *1,..,n*, которые будут соответствовать номерам вершин в графе H, после чего посетить все ребра восстанавливаемого графа, для того что бы установить номера вершин, которым инцидентно посещенное ребро, и, таким образом, установить какое ребро необходимо будет добавить в граф H.

Теорема 1. *Алгоритмы, реализующие построение нумерации на вершинах графа G и последующий обход всех ребер графа, строят граф H изоморфный графу G с точностью до меток на элементах графа.*

Теорема 2. *Для реализации эксперимента по восстановлению графа G агенту потребуетя n различных красок и не более чем* n^2 *ячеек памяти, где n количество вершин в графе G.*

На основе этого подхода можно получить множество алгоритмов для восстановления графа, основанных на построении на вершинах графа нумерации. Существует множество методов построения ну-

мераций на вершинах графа [4]. В силу ограничений наложенных на агента, наиболее простым для агента будет метод построения нумерации на вершинах графа M-нумерации [4]. M-нумерация — нумерация вершин при обходе графа методом в глубину.

Теорема 3. *Алгоритмы, реализующие построение M-нумерации на вершинах графа G, выполняют эксперимент по восстановлению графа за $2(n-1)+2(m-n+1)$ шагов, где m — количество ребер в графе G.*

В конкретных задачах по восстановлению графа может быть невозможно использование агентом различных красок в количестве n. Поэтому более приемлемым будет реализовывать нумерацию неявно, то есть, без присвоения явно номера вершине восстанавливаемого графа. Для агента будет проще всего реализовать постороение неявной M-нумерации. Применение неявной M-нумерации позволяет существенно сократить используемое количество различных красок, но ухудшает временную сложность, поскольку для получения явного номера вершины графа из неявного ему потребуется совершить некоторое количество шагов.

Алгоритмы предложенные в [2, 3] реализуют эксперимент по восстановлению графа при помощи построения на нем неявной M-нумерации.

Теорема 4. *Алгоритмы предложенные в* [2]*, реализуют построение неявной M-нумерации на вершинах графа G. Агент выполнит эксперимент по восстановлению графа не менее, чем за $O(n)$ и не более, чем за $O(n^2)$ шагов. При этом агент использует три различные краски и один камень.*

Теорема 5. *Алгоритмы предложенные в* [3]*, реализуют построение неявной M-нумерации на вершинах графа G. Агент выполнит эксперимент по восстановлению графа не менее, чем за $O(n)$ и не более, чем за $O(mn)$ шагов. При этом агент использует две различные краски.*

Таким образом, предложен общий подход к проведению эксперимента по восстановлению графа, заданного не классическим образом. Подход основан на построении нумерации на вершинах восстанавливаемого графа. Найдена нумерация, которая обеспечивает наименьшую временную сложность для времени проведения эксперимента по восстановлению графа, которое является линейной функцией от числа ребер в восстанавливаемом графе и при этом использует линейное, от числа вершин восстанавливаемого графа, количество различных красок. Предложены два алгоритма [2, 3], реализующие эксперимент по восстановлению графа при помощи построения на его вершинах неявной M-нумерации. Эти алгоритмы используют количество красок, не зависящее от количества вершин

в восстанавливаемом графе. Однако, алгоритмы не имеют точной оценки времени выполнения, чем если бы M-номера присваивались явно, и оценены снизу линейной функцией, а сверху квадратичной и кубической функциями, от числа вершин в исследуемом графе, соответственно.

Автор выражает благодарность Грунскому И. С. за советы и рекомендации при подготовке тезисов.

Список литературы

1. Dudek G., Jenkin M. Computational principles of mobile robotic. — Cambridge Univ. Press, 2000.

2. Грунский И. С., Татаринов Е. А. Алгоритм распознавания графов // Тр. 4 междунар. конф. "Параллельные вычисления и задачи управления". — М.: ИПУ РАН, 2008. — С. 1483–1498.

3. Грунский И. С., Татаринов Е. А. Распознавание конечного графа блуждающим по нему агентом // Вестник Донецкого университета. Серия А. Естественные науки. — 2009. — Вып. 1. — С. 492–497.

4. Касьянов В. Н., Евстигнеев В. А. Графы в программировании, визуализация и применение. — СПб.: БХВ—Петербург, 2003.

МЕТОДЫ СОВМЕЩЕНИЯ ЗАКОНОВ ФУНКЦИОНИРОВАНИЯ ДИСКРЕТНЫХ АВТОМАТОВ С ГЕОМЕТРИЧЕСКИМИ КРИВЫМИ

В. А. Твердохлебов (Саратов)

Замена конечных детерминированных автоматов дискретными детерминированными автоматами с бесконечным (счётным) множеством состояний принципиально расширяет область приложений автоматных моделей, в частности, включает в область приложений класс формально представляемых (например, машина Тьюринга) алгоритмов. Для такой замены требуется отказаться от традиционных способов задания автоматов (таблицами, графами, логическими уравнениями, формулами языка регулярных выражений) и разработать существенно новые средства представления законов функционирования автоматов. В статье рассматривается задание законов функционирования дискретных детерминированных автоматов дискретными математическими структурами, совмещёнными с геометрическими кривыми. Дискретный детерминированный автомат $A_{s_0} = (S, X, Y, \delta, \lambda, s_0)$, где S, X, Y — множества состояний, входных и выходных сигналов, а $\delta : S \times X \longrightarrow S$ и $\lambda : S \times X \longrightarrow Y$ — функции переходов и выходов, представим автоматным отображением

$\rho^A_{s_0} = \bigcup\limits_{p \in X^*} \{(p, \lambda(s,p))\}$, где X^* — множество всех входных последовательностей. Множество пар $\rho^A_{s_0} \subset X^* \times Y$ систематизируем введением линейных порядков ω_1 и ω_2 соответственно на множествах X^* и Y.

Множество пар $\rho^A_{s_0}$ представляем как множество точек в прямоугольной системе координат с осью абсцисс (X^*, ω_1) и осью ординат (Y, ω_2) и получаем дискретный график G_1. Каждой точке (p,y) графика G_1 сопоставляем в прямоугольной декартовой системе координат точку $(r_1(p), r_2(y))$, где $(r_1(p),\ r_2(y))$ — номера p и y по линейным порядкам ω_1 и ω_2.Полученный график G_2 точек с числовыми координатами можно совмещать с геометрическими кривыми, заданными аналитически, включая в такие кривые интерполяционные полиномы.

Следующие правила определяют линейный порядок ω_1 на X^*.

Правило 1. На множестве X вводим линейный порядок $x_1 \prec_1 x_2 \prec_1 \ldots \prec_1 x_k \prec_1 \ldots$

Правило 2. Порядок ω_1 на X распространим до линейного порядка на множестве X^*, полагая, что для любых слов $p_1, p_2 \in X^*$ неодинаковой длины $(p_1 \neq p_2)$ $|p_1| < |p_2| \to p_1 \prec_1 p_2$; для любых слов $p_1, p_2 \in X^*$, для которых $(p_1 \neq p_2)$ и $|p_1| = |p_2|$, их отношение по порядку ω_1 повторяет отношение ближайших слева несовпадающих букв слов p_1 и p_2.

Линейный порядок ω_2 для множества Y задается.

На основе размещения дискретных форм задания законов функционирования автоматов на непрерывных геометрических и числовых структурах, разработаны модели и методы: эффективного, компактного и точного задания дискретных автоматов с бесконечным множеством состояний, что эквивалентно заданию машин Тьюринга; распознавания автоматов по их наблюдаемому поведению на основе анализа геометрических кривых, соответствующих законами их функционирования; преобразования непрерывных геометрических кривых линий и последовательностей элементов конечных множеств в символьные и числовые графики, определяющие законы функционирования автоматов.

Представление автоматных отображений графиками вида G_1 и G_2 при фиксированных множествах X, Y и линейных порядках ω_1 и ω_2 позволяет взаимноднозначно представлять автоматные отображения последовательностями вторых координат графиков G_1 и G_2. Для оценки сложности автоматных отображений по сложности последовательностей вторых координат графиков разработан спектр Ω числовых показателей, характеризующих варианты определения последовательностей рекуррентными формами [1–3]. Спектр $\Omega(\xi)$ для последовательности имеет 5 уровней: $\Omega(\xi) =$

$(\Omega_0(\xi), \Omega_1(\xi), \Omega_2(\xi), \Omega_3(\xi), \Omega_4(\xi))$, на которых числовыми значениями представлены порядки рекуррентных форм, длины отрезков последовательности, определяемые отдельными рекуррентными формами и количества смен рекуррентных форм. По определению $\Omega_0(\xi) = m_0(\xi)$, где $m_0(\xi)$ — наименьший порядок рекуррентной формы, определяющей всю последовательность ξ. На уровне $\Omega_1(\xi)$ спектра $\Omega(\xi)$ расположено m_0 чисел ($m_0 \in N^+$), определяющих для рекуррентных форм порядков от 1 до m_0 размеры наибольших определяемых начальных отрезков последовательности ξ. Уровень $\Omega_2(\xi)$ содержит m_0 чисел, показывающих, сколько раз для рассматриваемого порядка рекуррентных форм потребовалось заменять рекуррентные формы при определении последовательности ξ. На уровне $\Omega_3(\xi)$ каждое число смен рекуррентных форм, показанное на уровне $\Omega_2(\xi)$, заменено длинами отрезков последовательности ξ, определяемых отдельными рекуррентными формами.

С использованием введенных обозначений спектр $\Omega(\xi)$ имеет структуру: $\Omega_0(\xi) = \langle m_0(\xi) \rangle$; $\Omega_1(\xi) = \langle (d^1(\xi), d^2(\xi), ..., d^\alpha(\xi)) \rangle$; $\Omega_2(\xi) = \langle (r^1(\xi), r^2(\xi), ..., r^\alpha(\xi)) \rangle$; $\Omega_3(\xi) = \langle (\Omega_3^1(\xi), \Omega_3^2(\xi), ..., \Omega_3^\alpha(\xi)) \rangle$, где $\alpha = m_0(\xi)$ и $\Omega_3^j(\xi) = \langle (d_1^j(\xi), d_2^j(\xi), ..., d_{n_j}^j(\xi)) \rangle$ (n_j — номер последнего отрезка в определении последовательности ξ как последовательности отрезков, определяемых отдельными рекуррентными формами порядка j); $\Omega_4(\xi) = \Theta(\Omega_3(\xi))$, где Θ — оператор замены в $\Omega_3(\xi)$ величин длин отрезков весами использованных рекуррентных форм для определения отрезков. Четвертый уровень $\Omega_4(\xi)$ спектра $\Omega(\xi)$ к характеристике последовательности ξ по количеству изменений правил, определяющих взаиморасположение элементов в последовательности, и величинам областей действия правил, представленной на уровнях $\Omega_1(\xi) - \Omega_3(\xi)$, добавляет оценки сложности самих правил. В достаточно общем случае можно вводить веса правил (рекуррентных форм) и веса конкретных реализаций правил, используемых при определении конкретных отрезков. Подробнее определение спектра см. в работах [1–2], а использование спектра для анализа свойств законов функционирования автоматов, определенных последовательностями, содержится в работе [4]. Определение последовательности рекуррентной формой F (или последовательностью рекуррентных форм) реализуется на основе совмещения переменных рекуррентной формы с элементами последовательности ξ по правилу: для любого $t, t > m$ (или t принадлежит рассматриваемому интервалу целых положительных чисел) $F(u(t-m), u(t-m+1), ..., u(t-1)) = u(t)$.

Представление автоматного отображения числовым графиком вида G_2 позволяет использовать классические методы интерполяции

для доопределения (точками на геометрической кривой) частично заданных автоматных отображений.

Список литературы

1. Твердохлебов В. А. Геометрические образы законов функционирования автоматов. — Саратов: Научная книга, 2008.

2. Твердохлебов В. А. Оценка сложности управления движением по известному маршруту // Проблемы управления. — 2009. — 5. — С. 69–73.

3. Твердохлебов В. А. Методы интерполяции в техническом диагностировании // Проблемы управления. — 2007. — 2. — С. 28–34.

4. Епифанов А. С. Анализ фазовых картин дискретных динамических систем. — Саратов: Научная книга, 2008.

О ЛИНЕЙНОМ ПО ВРЕМЕНИ КОНСТРУИРОВАНИИ ИЗОБРАЖЕНИЙ КЛЕТОЧНЫМ АВТОМАТОМ С ТРЕМЯ СОСТОЯНИЯМИ

Е. Е. Титова (Москва)

В работе рассматривается задача конструирования изображений клеточными автоматами на прямоугольном экране. В каждую клетку прямоугольного экрана $n \times m$ помещено по одному экземпляру одного и того же автомата $\mathcal{A}$ (клеточного), к его входам присоединены выходы автоматов, стоящих в соседних клетках, выход автомата — его текущее состояние. Доопределим нулями крайние входы автоматов n-й строки и m-го столбца. Неопределенные входы автоматов первой строки и первого столбца будем называть свободными входами, а всю эту конструкцию — (n, m)-*экраном* $S =< \mathcal{A}, n, m >$. Также имеется внешний автономный автомат $\mathcal{A}_e$ с $(n+m)$ выходами, который генерирует входные последовательности для свободных входов клеточных автоматов. Пара $G =< \mathcal{A}_e, S >$, состоящая из экрана и внешнего автомата называется *генератором*. *Изображением* называется матрица из нулей и единиц. $\Im(n, m)$ — множество всех изображений размера $n \times m$. (n, m)-экран S называется *универсальным*, если для любого изображения $\Im \in \Im(n, m)$ существует такой внешний автомат $\mathcal{A}_e$ (и тем самым такой генератор $G =< \mathcal{A}_e, S >$), что через некоторое время $T(\mathcal{A}_e, S)$ после начала работы внешнего автомата на экране появится изображение $\Im$, которое при подаче нулей на свободные входы остается неизменным сколь угодно долго. $\mathcal{U}(n, m)$ — множество всех универсальных (n, m)-экранов. Через

$\mathcal{G}(S, \Im)$ обозначим множество генераторов $< \mathcal{A}_e, S >$, формирующих изображение $\Im$.

Если $S =< \mathcal{A}, n, m >$ — экран, то $Q(S)$ — число состояний клеточного автомата $\mathcal{A}$,

$$Q(n,m) = \min_{S \in \mathcal{U}(n,m)} Q(S).$$

Обозначим

$$T(S, \Im) = \min_{<\mathcal{A}_e, S> \in \mathcal{G}(S, \Im)} T(\mathcal{A}_e, S),$$

$$T(S,n,m) = \max_{\Im \in \Im(n,m)} T(S, \Im),$$

$$T(n,m) = \min_{S \in \mathcal{U}(n,m)} T(S,n,m),$$

$$T(n,m,q) = \min_{S \in \mathcal{U}(n,m), Q(S) \le q} T(S,n,m).$$

Показано, что для любого изображения необходимо и достаточно, чтобы клеточный автомат имел 3 состояния. Получены оценки времени конструирования изображений в зависимости от числа состояний клеточного автомата.

Теорема 1. *Пусть* $n, m \in \boldsymbol{N}$. *Если* $\min(n,m) = 1$, *то* $Q(n,m) = 2$; *если* $n, m \ge 2$, *то* $Q(n,m) = 3$.

Теорема 2. *Для любых* $n, m \in \boldsymbol{N}$

$$T(n,m) = \min(n,m).$$

Теорема 3. *Если* $n, m \in \boldsymbol{N}$, $m, n \ge 2$, *то*

$$T(n,m,3) \le n + m + \min(n,m),$$

$$T(n,m,5) \le 2\min(n,m) + 2.$$

Теорема 3 означает, что существует генератор с тремя состояниями клеточного автомата, который строит любое изображение за линейное время, а именно за $n + m + \min(n,m)$. Однако, существует генератор с тремя состояниями клеточного автомата, для которого время конструирования изображения зависит от количества точек в изображении. В случае, если число k точек в изображении мало, этот генератор строит изображение быстрее первого.

Замечание. *Существует* (n,m)*-экран с клеточным автоматом из 3 состояний, который изображение, содержащее* $k \le mn$ *точек, строит за время* $\min(3k + n + m + 5, 3nm + 1)$.

Доопределим теперь нулями все свободные входы экрана кроме одного, первого в верхней строке. Соответственно внешний автомат имеет только один выход. Таким образом, теперь задача состоит в построении генератора, который строит любое наперед заданное изображение, используя только один свободный вход. Показано, что для этого достаточно чтобы клеточный автомат имел 8 состояний.

Теорема 4. *Если* $n, m \in \boldsymbol{N}$, $m, n \geq 2$, *то*

$$T(n, m, 8) \leq 2mn + 5.$$

Автор выражает искреннюю благодарность Э. Э. Гасанову за постановку задачи и научное руководство.

Список литературы

1. КудрявцевВ. Б. Функциональные системы. М.: Изд-во МГУ, 1982.

2. КудрявцевВ. Б., Подколзин А. С., Болотов А. А. Основы теории однородных структур. — М.: Наука, 1990.

3. Кудрявцев В. Б., Алешин С. В., Подколзин А. С. Введение в теорию автоматов. — М.: Наука, 1985.

МОДИФИКАЦИЯ ТРАНСФОРМАЦИОННОГО МЕТОДА

В. Е. Хачатрян, Я. Г. Великая (Белгород)

Трансформационный метод предназначен для распознавания эквивалентности моделей вычислений [1], в частности, позволяет распознать эквивалентность для некоторых классов многоленточных автоматов [2]. Уникальность метода заключается в том, что он позволяет распознать эквивалентность моделей в случае, когда проблема включения не разрешима [3]. Для определенности, под моделью будем понимать n-ленточный бинарный автомат [2]. При проверке моделей D_1 и D_2 на эквивалентность трансформационным методом выполняются следующие действия:

– для модели D_1 строится древовидное покрытие $D_1(\mathrm{F})$, остовное дерево [1], на котором указываются пары эквивалентных вершин $\mathrm{S}=\{(s_1,s'_1),\ldots,(s_k,s'_k)\}$ [2];

– модель D_2, эквивалентными фрагментными преобразованиями, перестраивается в новую модель D_3, которая начинается древовидным фрагментом D_3(F), изоморфным D_1(F). В случае невозможности построения такого фрагмента модели D_1 и D_2 являются не эквивалентными. Обозначим через S'=$\{(d_1, d'_1),\ldots,\ (d_k,d'_k)\}$ множество пар вершин, где d_i, s_i и d'_i ,s'_i соответствующие друг другу вершины. Соответсвие определено изоморфизмом древовидных фрагментов D_1(F) и D_3(F);

– на эквивалентность проверяются порожденные процессом подмодели $D_3(d_i)$,$D_3(d'_i)$, где i=1,2,...,k, а через $D_3(d_i)$,$D_3(d'_i)$ обозначены подмодели модели D_3, начинающиеся в состояниях d_i и d'_i соответственно;

– вышеописанные действия проверки на эквивалентность повторяются для всех вновь порожденных подмоделей;

– в процессе сравнения моделей строится дерево потомков T(D_1,D_2), вершины которого помечаются парами сравниваемых подмоделей. Корень помечается парой (D_1,D_2), вершины следующего яруса метками $(D_3(d_i), D_3(d'_i))$, где $i = 1, 2, \ldots, k$ и т. д.

Теорема 1 [1]. *Модели D_1 и D_2 эквивалентны тогда и только тогда, когда в дереве потомков существует конечное сечение, каждая метка которого состоит из пар эквивалентных моделей.*

В частности, модели будут эквивалентны, если такие пары будут состоять лишь из изоморфных моделей. Построение древовидного покрытия в общем случае неоднозначно. Неоднозначность имеет место в том случае, когда в модели D существуют состояния s_i, в которые из входа модели D, ведут различные простые пути. Тогда, для пары эквивалентных состояний (s_i, s'_i) состояния s_i и s'_i древовидного покрытия D(F) будут лежать на разных ветвях. Последнее означает, что, сравниваемые на эквивалентность на следующем шаге метода подмодели $D_3(d_i)$ и $D_3(d'_i)$, вообще говоря, задаются различными графами. Подмодели $D_3(d_i)$ и $D_3(d'_i)$ не имеют общих состояний. В случае, когда состояния s_i и s'_i находятся на одной ветви древовидного покрытия $D_1(F)$,причем вершина s_i предшествует вершине s'_i, где $i = 1, 2, \ldots, k$, обозначим как $s_i|s'_i$. Тогда соответствующие им состояния d_i, d'_i в модели D_3 также будут находиться на одной ветви, причем $d_i|d'_i$. Это означает, что подмодель $D_3(d'_i)$ является частью подмодели $D_3(d_i)$. Модель обладает однозначным

покрытием, если для любой пары эквивалентных вершин из списка S=$\{(s_1,s'_1),\ldots,(s_k,s'_k)\}$ выполняется условие $s_i \| s'_i$, где $i = 1, 2, \ldots, k$. В работе [4] описывается процедура γ, состоящая из эквивалентных преобразований для которой справедлива

Теорема 2. *Процедура γ по любой модели строит ей строго эквивалентную с однозначным покрытием.*

Модели считаются строго эквивалентными (автоматно- эквивалентными), если у них совпадают множества историй путей, ведущих из входа выход [2]. В работе [5] доказано, что при проверке моделей, являющихся строго эквивалентными, трансформационный метод может выдать, два типа сечений. Первый тип — это α-сечение, сечение все метки которого состоят из изоморфных пар моделей; второй тип — β-сечение, любая метка сечения повторяется в дереве потомков, причем на той же ветви.

При сравнении моделей D_1 и D_2, на строгую эквивалентность, предлагается модель D_2 предварительно минимизировать.

Теорема 3. *Если модели D_1 и D_2 строго эквивалентны, а D_2 является минимальной, тогда трансформационный метод распознает строгую эквивалентность этих моделей α-сечением.*

Модифицируем трансформационный метод следующим образом. При проверке на эквивалентность моделей, на любом шаге выполнения трансформационного метода, предварительно:

1) первую из сравниваемых моделей, преобразовать в эквивалентную ей однозначную модель;

2) вторую из сравниваемых моделей преобразовать в минимальную.

Предполагается, что предложенная модификация трансформационного метода позволит получить алгоритм разрешения эквивалентности многоленточных автоматов только за счет α-сечения.

Список литературы

1. Подловченко Р. И., Хачатрян В. Е. Метод трансформацинного распознавания эквивалентности в моделях вычислений // Материалы Восьмого Межд. сем. "Дискретная математика и ее приложения". — М., 2004. — С. 38–43.

2. Подловченко Р. И., Хачатрян В. Е. Об одном подходе к разрешению проблемы эквивалентности // Программирование. — 2004. — № 3. — С. 3–220.

3. Хачатрян В. Е., Великая Я. Г. О трансформационном методе распознавания эквивалентности // Труды восьмой международной конференции "Дискретные модели в теории управляющих систем". — М., 2009. — С. 202–206.

4. Хачатрян В. Е., Великая Я. Г. Модели вычислений с однозначным покрытием // Научные ведомости БелГУ". — 2009. — № 7. — С. 29–34.

5. Хачатрян В. Е. Трансформационный метод в моделях вычислений // Вестник компьютерных и информационных технологий. — 2008.—№ 4. —С. 52–355.

О ПРЕДЕЛЬНЫХ СВОЙСТВАХ РЕГУЛЯРНЫХ ЯЗЫКОВ

А. Б. Холоденко (Москва)

В настоящее время приложения — в том числе распознавание слитной речи — требуют простых и эффективных моделей естественных языков. Чаще всего для моделирования естественного языка используются вероятностые модели, в частности — n-граммные модели. К сожалению, их формальные свойства исследованы достаточно слабо. В данной работе предпринята попытка перенести свойства этих моделей на хорошо изученные регулярные языки, что позволяет не только лучше понять свойства вероятностных моделей, но и получить новые интересные результаты для самих регулярных языков.

В работе предложено обобщение понятия n-граммной модели на бесконечные формальные языки. Для этого в начале вводится частота встречаемости слова w на s-м месте, а затем рассматривается предельная частота встречаемости слова w как предел при s стремящемся к бесконечности.

Более точно:

Пусть $L(s)$ — множество слов языка L длины s; PL — множество префиксов слов языка L, включая сами слова; L_γ — множество слов языка L, оканчивающихся на слово γ.

Пусть $|w| = n$. Обозначим через $l_w(s)$ число слов языка L, имеющих с $(s-n+1)$-й по s-ю букву подслово w, то есть $l_w(s) = |PL_w(s)|$.

Обозначим через $G_w(s) = \frac{l_w(s)}{\sum\limits_{|w'|=|w|} l_{w'}(s)}$ частоту встречаемости слова w на s-м месте. Тогда $G_w = \lim\limits_{s\to\infty} G_w(s)$ — предельная частота встречаемости слова w среди всех слов той же длины.

Пусть $w \in A^*$, $a \in A$, $|wa| = n$. Введём величину $\Gamma_{w,a}$ как

$$\Gamma_{w,a} = \lim_{s\to\infty} \Gamma_{w,a}(s) = \lim_{s\to\infty} \frac{l_{wa}(s)}{\sum\limits_{|w'|=|w|} l_{w'a}(s)}.$$

Определение. Величину $\Gamma_{w,a}$, если она существует, назовём n-граммой языка L для пары (w, a).

Определение. Язык L назовём марковским языком порядка n, если существуют все n-граммы $\Gamma_{w,a}$, где $|wa| = n$ и существуют все частоты G_v, где $|v| = n$.

Множество марковских языков порядка n обозначим через $M(n)$; класс *марковских языков* обозначим через M.

Легко видеть, что не все регулярные языки являются марковскими, однако доля марковских языков среди всех регулярных языков велика. Если зафиксировать число состояний автомата, то отношение числа марковских языков, задаваемых автоматом с таким числом состояний к числу всех регулярных языков, обладающих тем же свойством будет не меньше чем $(1 - 1/e)$.

Классы марковских языков строго вкладываются друг в друга:

Теорема. *Если язык является марковским порядка n, то он также является марковским порядка k для любого $k < n$.*

Теорема. *Для любого $n \in \mathbb{N}$ существует язык L, такой, что $L \in M(n-1)$, но при этом $L \notin M(n)$.*

Таким образом, марковские языки образуют строго сужающуюся последовательность: $M(1) \supset M(2) \supset M(3) \supset \ldots \supset M(n) \supset \ldots \supset M$.

С другой стороны, если язык L фиксирован, то цепочка вложений для него обрывается на конечном шаге и становится возможным установить его принадлежность к классу марковских языков за конечное число шагов.

Теорема. *Если язык $L_{\mathfrak{A}}$ задан автоматом $\mathfrak{A} = \{A, Q, \varphi, Q_F, q_0\}$, то из $L_{\mathfrak{A}} \in M(2^{|Q|})$ следует, что $L_{\mathfrak{A}} \in M$.*

Любая n-грамма может быть вычислена по диаграмме переходов автомата, однако это требует умения находить собственные числа для матриц большой размерности.

Оказывается, что класс всех марковских языков не замкнут относительно основных теоретико-языковых операций: объединения, пересечения и дополнения, поэтому имеет смысл ввести в рассмотрение более узкие замкнутые классы марковских языков. Примером такого класса является класс *каскадно-дефинитных языков*, получаемый из класса дефинитных языков при помощи рекурсивного применения операции склейки двух автоматов.

Пусть $\mathfrak{A}^1 = (A, Q^1, \varphi^1, Q^1_F, q^1_0)$, $\mathfrak{A}^2 = (A, Q^2, \varphi^2, Q^2_F, q^2_0)$ — конечные детерминированные автоматы. Пусть также $q^1 \in Q^1$ и $q^2 \in Q^2$.

Определение. Результатом склейки автоматов $\mathfrak{A}^1$ и $\mathfrak{A}^2$ называется автомат

$$\mathfrak{A} = (A, Q^1 \cup Q^2 \setminus \{q^1\}, \varphi, Q^1_F \cup Q^2_F \setminus \{q^1\}, q^1_0), \text{ где}$$

$$\varphi(q,a) = \begin{cases} \varphi^1(q,a) & \text{если } q \in Q^1 \setminus \{q^1\} \text{ и } \varphi^1(q,a) \neq q^1 \\ q^2 & \text{если } q \in Q^1 \setminus \{q^1\} \text{ и } \varphi^1(q,a) = q^1 \\ \varphi^1(q^2,a) & \text{если } q = q^1 \\ \varphi^2(q,a) & \text{если } q \in Q^2. \end{cases}$$

Оказывается, введённая таким образом операция склейки двух автоматов по паре состояний позволяет получать автоматы с заданными свойствами из набора простейших автоматов: "циклов" и "отрезков".

Утверждение. *Множество $\{G_{ab}\}$ является системой биграмм для языка L тогда и только тогда, когда для любого i выполнено: $\Sigma_i \geq M_i$, где Σ_i — сумма по i-му столбцу, а M_i — максимум по i-й строке в матрице переходов для автомата, задающего язык L.*

Определение. Введённое выше условие будем называть условием биграммности множества $\{G_{ab}\}$, а соответствующую ей матрицу π будем называть биграммной матрицей.

Теорема. *Для всякой рациональной биграммной матрицы π найдётся автомат $\mathfrak{A}$, матрица биграмм которого $\pi_{\mathfrak{A}}$ будет в точности совпадать с исходной биграммной матрицей π, и который может быть получен из "простейших" автоматов — "отрезков" и "циклов" путём применения к ним операции склейки автоматов.*

Очевидно, что в случае иррациональной биграммной матрицы она может быть приближена рациональной с любой заданной точностью. Таким образом, для произвольной биграммной матрицы может быть (конструктивно) построен автомат $\mathfrak{A}'$, имеющий биграммную матрицу, сколь угодно близкую к заданной.

Список литературы

1. Холоденко А. Б. О построении статистических языковых моделей для систем распознавания русской речи // Интеллектуальные системы. — 2002. — Т. 6, вып. 1–4. — С. 381–394.

2. Бабин Д. Н., Холоденко А. Б. Об автоматной аппроксимации естественных языков // Интеллектуальные системы. — 2008. — Т. 12, вып. 1–4. — С. 125–136.

3. Холоденко А. Б. О марковских регулярных языках // Материалы IX Международного семинара «Дискретная математика и её

приложения», посвященного 75-летию со дня рождения О. Б. Лупанова (18–23 июня 2007 года). — М.: Изд-во мех-мат ф-та МГУ, 2007. — С. 358–361.

ОБ А-ПОЛНОТЕ И ПОЛНОТЕ В КЛАССЕ ЛИНЕЙНО-АВТОМАТНЫХ ФУНКЦИЙ НАД ПРОСТЫМИ КОНЕЧНЫМИ ПОЛЯМИ

А. А. Часовских (Москва)

В работе [1] решены задачи А-полноты и полноты для класса линейно-автоматных функций над полем $E_2 = \{0, 1\}$. В настоящей работе эти результаты обобщены для линейно-автоматных функций над полем E_p, $E_p = \{0, 1, \ldots, p-1\}$, где p — простое число.

Зафиксируем простое число p. Через $E_p[\xi]$ обозначим множество всех многочленов переменной ξ над полем E_p. Для множества всех многочленов из $E_p[\xi]$ с ненулевым свободным членом будем использовать обозначение $E'_p[\xi]$. Поле отношений многочленов из $E_p[\xi]$ принято обозначать $E_p(\xi)$, а его подкольцо

$$\left\{ \frac{u(\xi)}{v(\xi)} \mid u(\xi) \in E_p[\xi], v(\xi) \in E'_p[\xi] \right\}$$

будем обозначать $E'_p(\xi)$. Множество всех формальных рядов переменной ξ с коэффициентами из E_p будем обозначать $R_p(\xi)$.

Пусть n — натуральное число. Отображение $f(x_1, \ldots, x_n)$ из $R_p^n(\xi)$ в $R_p(\xi)$ называется линейно-автоматной функцией (л.-а. функцией) над E_p, если найдутся μ_i, $\mu_i \in E'_p(\mu)$, $i = 0, 1, \ldots, n$, такие, что для любых α_i, $\alpha_i \in R_p(\xi)$, $i = 1, 2, \ldots, n$, выполнено равенство $f(\alpha_1, \alpha_2, \ldots, \alpha_n) = \sum_{i=1}^{n} \mu_i \alpha_i + \mu_0$, где операции "$+$" и "$\cdot$" индуцированы операциями в E_p. Поэтому л.-а. функция $f(x_1, \ldots, x_n)$ задается выражением $\sum_{i=1}^{n} \mu_i x_i + \mu_0$.

Множество всех л.-а. функций над E_p обозначим L_p. В классе L_p рассмотрим аппроксимационный оператор замыкания A [2], а также оператор замыкания по операциям композиции [3] (стр. 161).

Обозначим через $U(f)$ множество $\{\mu_i(\xi)|i=1,2,\ldots,n\}$. Для множества M, $M \subseteq L_p$, положим

$$U(M) = \cup_{f\in M} U(f).$$

Переменную x_i функции f, $f = \sum_{i=1}^{n} \mu_i x_i + \mu_0$, будем называть существенной, если $\mu_i \neq 0$. Переменную x_j этой функции будем называть непосредственной, если $\mu_j \notin \{\xi\}E'_p(\xi)$. Рассмотрим следующие множества л.-а. функций.

Пусть $k \in E_p$,

$$T_k = \{f \mid f \text{ сохраняет } k \text{ в начальный момент}\},$$

$$V_1 = \{\ f \mid f \text{ имеет не более одной непосредственной переменной}\},$$

$$V_p = \{\ f \mid \text{сумма свободных членов рядов из } U(f) \text{ по модулю } p \text{ сравнимо с } 1\},$$

$$M\left(\xi^2\right) = \{\ f \mid f \text{ не зависит от входа в момент времени, следующий за начальным}\}.$$

Через AJ_p обозначим следующее множество классов л.-а. функций.

$$AJ_p = \left\{\ V_1, V_p, M\left(\xi^2\right), T_k \mid k = 0,1,\ldots,p-1\right\}.$$

Теорема 1. *Множество AJ_p является приведенной А-критериальной системой А-предполных в L_p классов.*
А-предполных классов в L_p, не содержащихся в AJ_p, не существует.

Введем некоторые обозначения. Пусть л.-а. функции $f(x_1, x_2, \ldots, x_n)$, удовлетворяет равенству $f = \sum_{i=1}^{n} \mu_i x_i + \mu_0$.

Положим

$$M_0^{(1)} = \left\{\ \tfrac{u(\xi)}{v(\xi)} \mid u(\xi) \in E_p[\xi], v(\xi) \in E'_p[\xi], \text{ найдется } a, a \in E_p, \text{ что } \deg(u(\xi) - av(\xi)) < \deg v(\xi), \text{ и } u(\xi) - av(\xi) \in \{\xi\} \cdot E_p[\xi]\right\},$$

$$M_i^{(1)} = \left\{\ \tfrac{u(\xi)}{v(\xi)} \mid u(\xi) \in E_p[\xi], v(\xi) \in E'_p[\xi], \text{ найдется } a, a \in E_p, \text{ что } \xi p_i(\xi) | u(\xi) - av(\xi)\right\},\ i = 1,2,\ldots,$$

$$R_0^{(1)} = \left\{ \tfrac{u(\xi)}{v(\xi)} \mid u(\xi) \in E_p[\xi], v(\xi) \in E_p'[\xi],\ \deg u(\xi) < \deg v(\xi) \right\},$$

$$R_i^{(1)} = \left\{ \tfrac{u(\xi)}{v(\xi)} \mid u(\xi) \in E_p[\xi],\ v(\xi) \in E_p'[\xi], \right.$$
$$\left. (u(\xi), v(\xi)) = 1,\ p_i(\xi) | u(\xi) \right\},\ i = 1, 2, \ldots,$$

$$\tilde{R}_0^{(1)} = \left\{ \mu | \mu \in E'(\xi), \mu = \frac{u}{v}, \deg u \le \deg v \right\},$$

$$\tilde{R}_i^{(1)} = \left\{ \mu | \mu \in E'(\xi), \mu = \frac{u}{v}, (v, p_i) = 1 \right\},\ i = 2, 3, \ldots,$$

$$M_i = \left\{ f |\ f \in L_p,\ U(f) \subset M_i^{(1)} \right\},\ i = 0, 1, \ldots,$$

$$R_i^{\text{с}} = \Big\{ f \mid f \in L_p, \text{ для любого } \mu, \mu \in U(f), \text{ выполнено}$$

$$\mu \in \tilde{R}_i^{(1)}, \text{ если } \mu \text{ соответствует единственной существенной}$$

$$\text{переменной } f, \text{ и } \mu \in R_i^{(1)}, \text{ в противном случае} \Big\},$$

$$R_i^{\text{н}} = \Big\{ f |\ f \in L_p, \text{ для любого } \mu, \mu \in U(f), \text{ выполнено}$$

$$\mu \in \tilde{R}_i^{(1)}, \text{ если } \mu \text{ соответствует единственной непосредствен-}$$

$$\text{ной переменной } f, \text{ и } \mu \in R_i^{(1)}, \text{ в противном случае} \Big\}.$$

Через J_p обозначим множество

$$\{T_0, T_1, \ldots, T_{p-1}, V_1, V_p, M_i,\ i = 0, 1, \ldots,\ R_j^{\text{с}}, R_j^{\text{н}},\ j = 0, 2, 3, \ldots\}.$$

Теорема 2. *J_p — критериальная система в L_p, состоящая из предполных классов и любой предполный в L_p класс содержится в J_p.*

Теорема 3. *Проблемы полноты и A-полноты конечных подмножеств из L_p алгоритмически разрешимы.*

Список литературы

1. Часовских А. А. О полноте в классе линейных автоматов // Математические вопросы кибернетики. Вып. 3. — М.: Наука, 1991. — С. 140–166.

2. Буевич В. А. Об алгоритмической неразрешимости распознавания А-полноты для о.-д. функций // Математические заметки. — 1972. — Вып. 6.
3. Кудрявцев В. Б., Алешин С. В., Подколзин А. С. Элементы теории автоматов. — М.: Изд-во МГУ, 1978.

ОЦЕНКИ ПРИБЛИЖЕНИЯ НЕПРЕРЫВНЫХ ФУНКЦИЙ КОНЕЧНЫМИ АВТОМАТАМИ

А. Н. Черепов (Смоленск)

Задача об оценке сложности реализации непрерывных функций и классов таких функций дискретными функциями близкими к автоматным, была поставлена А. Н. Колмогоровым. В технике часто используются устройства,фукционирующие следующим образом: на вход устройства последовательно поступают двоичные разряды информации,а само устройство реализует некоторую функцию. Примером таких устройств являются устройства подключенные к последовательному порту компьютера. Очевидно, что не все функции могут быть реализованы устройствами аналогичными классическим конечным автоматам, то есть выдавать на выходе устройства двоичный разряд результата сразу после появления значения соответствующего разряда на входе. В работах [1–3], в качестве множества приближающих функций рассматривался класс дискретных детерминированных функций с задержкой. Этот класс появляется при естественном обобщении понятия детерминированной функции.Был получен ряд результатов о сложности приближения некоторых функций детерминированными с задержкой, где сложность определялась как минимальное значение задержки. В работе [4] приведены аналогичные результаты для сложности, понимаемой как число состояний конечного автомата, приближающего функцию.

Рассмотрим множество всех бесконечных двоичных последовательностей E. Множество всех функций вида $f : E^n \to E$ обозначим P. Предположим, что $a_1, a_2, \ldots, a_n$ — последовательности из E, а $\tilde{a} = (a_1, a_2, \ldots, a_n)$ — набор таких последовательностей. Пусть $a_1|k, a_2|k, \ldots, a_n|k$ — первые k членов последовательностей $a_1, a_2, \ldots, a_n$ соответственно, тогда $\tilde{a}|k = (a_1|k, a_2|k, , a_n|k)$.

Определение 1 [3]. Говорим, что функция f является детерминированной функцией с задержкой τ, где τ — произвольное неотрицательное целое число, если для любого $k = 1, 2, 3, \ldots$ и любых $\tilde{a}, \tilde{b}$ выполнено:

$$\tilde{a}|k + \tau = \tilde{b}|k + \tau \Rightarrow f(\tilde{a})|k = f(\tilde{b})|k.$$

При $\tau = 0$ это определение совпадает с обычным определением детерминированной функции.

Множество детерминированных функций с задержкой можно определить и следующим образом.

Определение 2. Говорим, что функция f является детерминированной функцией с задержкой τ, где τ — произвольное неотрицательное целое число, если существует такая детерминированная функция g, что для любого $\tilde{a}$ и $b = g(\tilde{a})$, $b = b(1)b(2)b(3)\ldots$ значение функции f на наборе $\tilde{a}$ равно $f(\tilde{a}) = b(\tau + 1)b(\tau + 2)b(\tau + 3)\ldots$

Определение 3. Назовем конечным автоматом с задержкой τ конечный автомат, который при подаче на его входы некоторых входных последовательностей начинает формировать выходную последовательность не с первого момента времени, а с некоторой задержкой, не превосходящей τ.

Перейдем к вопросу о возможности реализации непрерывных функций, осуществляющих отображение точек n-мерного единичного куба на отрезок [0,1]. Сопоставим каждой двоичной последовательности $a(1)a(2)\ldots a(i)\ldots$ некоторое число отрезка $[0, 1]$, равное $0, a(1)a(2)\ldots a(i)\ldots$. Из двух возможных представлений

$$0, a(1)a(2)\ldots a(i)100\ldots = 0, a(1)a(2)\ldots a(i)0111\ldots$$

выберем первое. Для числа 1 берется представление $1 = 0, 1111\ldots$.

Определение 4. Пусть $\varepsilon > 0$, будем говорить, что функция $d(\tilde{x})$ ε-равна функции $f(\tilde{x})$ на единичном кубе $[0, 1]^n$, если при любом $\tilde{x} \in [0, 1]^n$ имеем, что $\mid f(\tilde{x}) - d(\tilde{x}) \mid < \varepsilon$. Будем также говорить, что в этом случае $d(\tilde{x})$ ε-приближает $f(\tilde{x})$. Если функция $d(\tilde{x})$ ε-приближает $f(\tilde{x})$ и соответствует дискретной функции, реализуемой конечным автоматом A с задержкой τ, то будем говорить, что автомат A ε-приближает $f(\tilde{x})$.

Теорема 1 [1]. *Для любого ε и любой функции $f(\tilde{x}) \in C(I^n)$ существует натуральное число τ и функция $d(\tilde{x}) \in D_d^\tau$ такие, что $d(\tilde{x})$ ε-равна $f(\tilde{x})$.*

Не всякую непрерывную функцию можно ε-приблизить обычным конечным автоматом, так как не всякую непрерывную функцию

можно ε-приблизить детерминированной функцией [3]. Но конечных автоматов с задержкой уже достаточно.

Теорема 2 [4]. *Для любого $\varepsilon > 0$ и любой функции $f(\tilde{x}) \in C[0,1]^n$ существует число $\tau \geq 0$ и конечный автомат A с задержкой τ такие, что автомат A ε-приближает $f(\tilde{x})$.*

В заключение автор выражает свою благодарность В. А. Буевичу за постановку задачи.

Список литературы

1. Черепов А. Н. Оценки сложности приближения непрерывных функций некоторых классов детерминированными функциями с задержкой // Синтез и сложность управляющих систем. Сборник трудов 16 Международной школы-семинара. — М.: Изд-во механико-математического факультета МГУ, 2006. — С. 118–122.

2. Черепов А. Н. О сложности приближения непрерывных функций детерминированными функциями с задержкой // Интеллектуальные системы и компьютерные науки. Материалы 9 Международной конференции. — М.: Изд-во механико -математического факультета МГУ, 2006. — С. 307–310.

3. Черепов А. Н. Оценки сложности приближения непрерывных функций некоторых классов детерминированными функциями с задержкой // Дискретная математика. — 2008. — Т. 20, вып. 4. — С. 147–156.

4. Черепов А. Н. Приближение непрерывных функций конечными автоматами // Дискретные модели в теории управляющих систем. Труды 8 Международной конференции. — М.: МаксПресс, 2009. — С. 339–343.

АВТОМАТНАЯ МОДЕЛЬ ЛЕГКИХ БЕЗ ПАТОЛОГИЙ

Ю. Г. Чернова (Москва)

В работе строится автоматная модель процесса транспортировки вещества в легких, не имеющих патологических изменений, и изучаются свойства этой модели.

Оказалось, что процесс транспортировки можно достаточно адекватно представить некоторым структурным автоматом.

Рассмотрены две основные ситуации, когда легкие функционируют в чистой среде, а также, когда эта среда не является таковой. В обоих случаях решены задачи времени самоочищения, описания стартовых и финальных состояний соответствующего автомата, найдены критерии переводимости одного состояния в другое, построены семейства попарно непереводимых друг в друга состояний, оценены все основные параметры, характеизующие указанные задачи.

Рассмотрения чистой среды успешно распространены на случай загрязненной, но стационарной среды. Описаны все такие среды, в которых легкие функционируют с заданной долей допустимого загрязнения. Это описание получено как с помощью комбинаторных средств, так и с помощью средств алгебры языков. Рассмотрения модели для стационарных сред удалось распространить на случай легких в переменных по загрязнению средах. Выяснилось, что полученые для предыдущих случаев результаты с помощью "склеивающих" процедур алгебро-алгоритмического характера позволяют практически полностью описать структурный автомат, адекватный функционированию легких в переменно-загрязненных средах и решить весь цикл упомянутых задач для этого общего случая.

Автор выражает благодарность Кудрявцеву Валерию Борисовичу и Чучалину Александру Григорьевичу за постановку задачи и научное руководство.

Список литературы

1. Кудрявцев В. Б., Алешин С. В., Подколзин А. С. Введение в теорию автоматов. — М.: Наука, 1985.

2. Гераськина (Чернова) Ю. Г. Об одной автоматной модели в биологии // Дискретная математика. — 2007. — Т. 19, вып. 3. — С. 122–139.

3. Гераськина (Чернова) Ю. Г. Автоматная модель транспортировки вещества по легким в загрязненных стационарных средах // Интеллектуальные системы. — 2008. — Т. 12, вып. 1–2. — С. 151–179.

4. Гераськина (Чернова) Ю. Г. О стартовых состояниях автоматной модели легких в чистой среде // Дискретная математика. — 2008. — Т. 20, вып. 3. — С. 119–135.

5. Гераськина (Чернова) Ю. Г. Автоматная модель транспортировки вещества по легким в загрязненных средах // Интеллектуальные системы. — 2008. — Т. 12, вып. 1–4. — С. 179–210.

ЭКСПЕРТНАЯ СИСТЕМА ЭКСПРЕССНОЙ ОЦЕНКИ ЗОЛОТОРУДНЫХ МЕСТОРОЖДЕНИЙ НА ОСНОВЕ ВЫБОРА ОБЪЕКТОВ-АНАЛОГОВ И КОГНИТИВНОЙ ГРАФИКИ

И. А. Чижова, М. М. Константинов, С. Ф. Стружков (Москва), Д. А. Покровский (Париж)

Проблема поиска геологического объекта (месторождения), наиболее сходного с анализируемым по некоторым критериям, всегда интересовала исследователей. Пути ее решения различны. Но особенно интересен подход автоматизированного поиска по различным мерам сходства, дающим количественный показатель. По найденному среди хорошо изученных эталонных объектов ближайшему аналогу по методу аналогии возможна оценка неизвестных свойств экспертируемого объекта. Учитывая огромные возможности когнитивных (т. е. способствующих познанию) свойств графической информации, целесообразно ее использование при экспресс-оценке месторождений, поскольку на эталонном объекте обеспечивается наглядное представление признаков и геологических ситуаций, неизвестных на слабоизученном объекте. Впервые система экспресс-оценки золоторудных месторождений на основе выбора объекта-аналога дополнена графической базой данных, содержащей геологические материалы, необходимые при анализе месторождений, но которые невозможно представить в текстовом или цифровом виде. Учитывая широкое развитие интернет-технологий, для системы управления была выбрана технология создания вложенных HTML-файлов, обеспечивающая хранение неограниченного числа растровых изображений.

В научных исследованиях, в том числе и в фундаментальных, на стадиях формализации задачи, разработки моделей анализируемых объектов, схем применения методов решения, изображения полученных результатов для наглядности всегда применялась графическая информация (карты, схемы, разрезы, графики и т. д.). Современные технические возможности позволяют хранить, быстро находить необходимую информацию и сравнивать ее между собой.

Когнитивное компьютерное моделирование определяется как синтез традиционного компьютерного моделирования и когнитивной компьютерной графики. Под термином когнитивная графика понимается совокупность приемов и методов образного представления условий задачи, которое позволяет либо сразу увидеть решение, либо получить подсказку для его нахождения.

В предисловии к работе (Зенкин, 1991) Д. А. Поспелов сформулировал три основные задачи когнитивной компьютерной графики.

Первой задачей является создание таких моделей представления знаний, в которых было бы возможно однообразными средствами представлять как объекты, характерные для логического мышления, так и образы-картины, с которыми оперирует образное мышление. Вторая задача — визуализация тех человеческих знаний, для которых пока невозможно подобрать текстовые описания. Третья — поиск путей перехода от наблюдаемых образов-картин к формулировке некоторой гипотезы о тех механизмах и процессах, которые скрыты за динамикой наблюдаемых картин. Мы имеем дело, в основном, со второй задачей.

Унификация и стандартизация в представлении иллюстративной графической информации (растровых изображений) позволяет усилить ее когнитивные свойства, поскольку в данной ситуации упрощается процедура ее анализа при сопоставлении.

Учитывая огромные возможности когнитивных свойств графических образов, авторы приступили к созданию графической базы данных для информационно-аналитических системы экспресс-оценки золоторудных месторождений на основе выбора объекта-аналога. Такая база спроектирована как составная часть системы АНАЛОГ, разработанной авторами в 2002–2006 гг. Основной задачей, решаемой системой, является следующая: по комплексу признаков, имеющихся на экспертируемом объекте, найти наиболее сходный с ним объект из множества эталонов (хорошо изученных золоторудных месторождений), имеющихся в базе данных. Оценка экспертируемого объекта (определение его рудно-формационного типа, масштабности оруденения) проводится по методу аналогии на основании знаний об эталонном объекте-аналоге.

Изначально система АНАЛОГ опиралась на фактографическую базу данных. На сегодняшний день она содержит описание 247 золоторудных месторождений Мира в системе 894 признаков, объединенных в 26 групп. Графическая информация позволяет визуализировать ту часть человеческих знаний об объекте, для которых пока нет возможности получить текстовые описания. Разработан блок графического банка данных, содержащий растровую информацию по объектам-эталонам (карты, схемы, геологические разрезы, фото образцов и т. п.).

Этот блок носит прежде всего иллюстративный характер. Но его включение в систему обусловлено тем, что в ходе анализа информации по ближайшему объекту-аналогу у исследователя возникает новое знание моделируются возможные геологические ситуации для экспертируемого объекта. Если иллюстративная функция компьютерной графики заключается в отображении в более или менее адекватном визуальном оформлении того, что известно, то распростра-

нение знания по методу аналогии на экспертируемый объект носит когнитивный ха рактер и способствует интеллектуальному процессу получения этого знания на основе профессиональной интуиции.

Выбор способа вычисления меры сходства объектов (эталонов из базы данных и экспертируемого объекта) проводится в зависимости от вида используемой информации, которая может носить как качественный, так и количественный характер (Чижова, 2004). В качестве меры сходства между объектами используется модификация меры сходства Говера с учетом природы исходной информации. Сравнение экспертируемого объекта с объектами выборки проводится последовательно для каждой выбранной группы признаков.

В зависимости от формы представления исходной информации об объекте исследования меняются процедуры их анализа.

Список литературы

1. Зенкин А. А. Когнитивная компьютерная графика. — М.: Наука, 1991.

2. Чижова И. А. Технология создания информационно-аналитических систем для прогнозно-металлогенических исследований перспективных площадей // Проблемы рудной геологии, петрологии, минералогии и геохимии. — М.: ИГЕМ РАН, 2004. — С. 524–533.

3. Chizhova I. A., Konstantinov M. M., Strujkov S. F., Pokrovsky D. A. Economic-geological estimation of gold and ore deposits using information-analitical system for the selection of analogues // Natural Resources Research. — 2005. — V. 14, № 4. — P. 325–332.

О СЛОИСТОСТИ БУЛЕВЫХ ФУНКЦИЙ И ФУНКЦИЙ k-ЗНАЧНОЙ ЛОГИКИ

Т. С. Членова (Москва)

Введем понятие слоистости функций k-значной логики над полными системами в P_k, а также слоистости полных систем в P_k.

Пусть $G = \{g_1, \ldots, g_n\}$ — полная система в $P_k, k \geq 2$. Назовем блоком B над $\{g_i\}$ произвольную схему с одним выходом над $\{g_i\}$. Пусть, далее, $G_i = \{B | B-$ блок над $\{g_i\}\}$ и $\widetilde{G} = \cup_i G_i$.

Пусть ϕ — схема над системой G. Она также является и схемой над $\widetilde{G}$. Пусть в ϕ есть подсхема, являющаяся блоком B из множества $\widetilde{G}$. Тогда заменим эту подсхему на элемент B множества $\widetilde{G}$. При

этом получим схему ψ_1 над $\widetilde{G}$. Строим последовательность множеств $\Psi_0 = \{\psi_0\}$, $\Psi_1 = \{\psi_0, \psi_1\}$, $\Psi_2 = \{\psi_0, \psi_1, \psi_2\}$,..., $\Psi_p = \{\psi_0, \psi_1, ..., \psi_p\}$ схем над $\widetilde{G}$, где $\psi_0 = \phi$. Схема $\psi_i \in \Psi_i$ получается из какой-то схемы множества Ψ_{i-1} заменой некоторой ее подсхемы на блок из $\widetilde{G}$. Так как схема ϕ содержит конечное число элементов, то процесс построения прервется. Легко видеть, что результирующее множество Ψ не будет зависеть от самого процесса построения. Ψ назовем множеством представлений схемы ϕ над $\widetilde{G}$

Определение 1. Слоистостью схемы ϕ с одним выходом над полной системой G в $P_k, k \geq 2$, назовем число $S_G(\phi) = \min_{\psi \in \Psi} l(\psi)$, где $l(\psi)$ — глубина схемы ψ, а Ψ — множество представлений схемы ϕ над $\widetilde{G}$.

Определение 2. Слоистостью функции $f \in P_k$ над полной системой G в $P_k, k \geq 2$ называется число $S_G(f) = \min_{\phi \in \Phi} S_G(\phi)$, где Φ — множество всех схем, реализующих функцию f над системой G.

Определение 3. Слоистостью полной системы G, в P_k, $k \geq 2$ будем называть максимум слоистостей всех функций $f \in P_k$ над G , если множество чисел $\{S_G(f) | f \in P_k\}$ ограничено. Если это множество чисел является неограниченным, то будем считать слоистость системы равной бесконечности.

Наша цель — исследование слоистостей полных системы в $P_k, k \geq 2$. Начнем со случая P_2.

Рассмотрим сначала случай полных систем из P_2, состоящих из функций, зависящих от двух переменных.

Для этого случая верна теорема:

Теорема 1. *Любая полная система G в P_2^2, имеет слоистость, не превышающую* 4. *Существует полная система, в P_2^2, слоистость которой равна* 4.

Далее рассмотрим произвольные полные системы в P_2.

Можно доказать следующую теорему:

Теорема 2. *Любая полная система G в P_2, имеет слоистость, не превышающую* 5.

Перейдем к исследованию случая $P_k, k \geq 3$.

Определение 4. Система Слупецкого в $P_k, k \geq 3$, — система, состоящая из всех функций, зависящих от одной переменной, и существенной функции, принимающей все k значений.

Система Слупецкого в $P_k, k \geq 3$, является полной (теорема Слупецкого).

Теорема 3. *Пусть G — полная система в $P_k, k \geq 3$. Если в G есть существенная функция $g(x_1, \ldots, x_n)$, принимающая все k*

значений, такая, что соответствующая ей система Слупецкого имеет конечную слоистость, то слоистость системы G конечна.

Следующая теорема показывает, что для любого k в P_k существует достаточно широкий класс существенных функций, принимающих все k значений, таких, что соответствующие им системы Слупецкого имеют конечную слоистость.

Теорема 4. *Пусть G — система Слупецкого в $P_k, k \geq 3$, $g(x_1, \ldots, x_n) \in G$ — существенная функция, принимающая k значений. Пусть существуют номера i и j, $i < j$, $i, j \in [1, n]$, а так же набор $(\alpha_1, \ldots, \alpha_{i-1}, \alpha_{i+1}, \ldots, \alpha_{j-1}, \alpha_{j+1}, \ldots, \alpha_n)$, $\alpha_s \in Z_k$, такой, что $g(\alpha_1, \ldots, \alpha_{i-1}, x_i, \alpha_{i+1}, \ldots, \alpha_{j-1}, x_j, \alpha_{j+1}, \ldots, \alpha_n) = \max(x_i, x_j)$ при $x_i, x_j \in \{0, 1\}$. Тогда система G имеет конечную слоистость.*

Введем понятие площади схемы над полной системой в P_k.

Определение 5. Пусть ϕ — схема над полной системой G в P_k. Площадью схемы ϕ назовем число $M_G(\phi) = \min_{\psi \in \Psi} N(\psi)$, где Ψ — множество схем, являющихся всевозможными представлениями схемы ϕ блоками из $\widetilde{G}$, а $N(\psi)$ — количество блоков в схеме ψ.

Определение 6. Площадью функции $f \in P_k$, над полной системой G в P_k называется число $M_G(f) = \min_{\phi \in \Phi} M_G(\phi)$, где Φ — множество всех схем, реализующих функцию f над системой G таких, что их слоистость равна слоистости функции f.

Определение 7. Площадью полной системой G в P_k называется функция $M_G(n) = \max_{f \in P_k^{(n)}} M_G(f)$.

Для случая булевых функций верна следующая теорема.

Теорема 5. *Существуют полные системы G в P_2 такие, что при всех натуральных n $M_G(n) \geq \frac{2^n}{n+1}$.*

Замечание. Существуют полные системы в P_2, имеющие ограниченную площадь.

Список литературы

1. Яблонский С. В. Введение в дискретную математику. — М.: Высшая школа, 2003.

2. Лупанов О. Б. О синтезе некоторых классов управляющих систем // Проблемы кибернетики. — 1963. — Вып. 10. — С. 63–97.

3. Касим-Заде О. М. О глубине булевых функций при реализации схемами над произвольным базисом // Вестник Московского университета. Сер. 1. Математики. Механика. — 2007. — № 1. — С. 18–21.

4. Колмогоров А. Н. О представлении непрерывных функций нескольких переменных в виде суперпозиции непрерывных функций одного переменного и сложения // Избранные труды. Математика и механика. — М.: Наука, 1985. — С. 340–344.

5. Половников В. С. О некоторых характеристиках нейронных схем // Интеллектуальные системы. — 2004. — Т. 8. — С. 121–145.

ОЦЕНКИ ВРЕМЕННÓЙ СЛОЖНОСТИ САМОКОРРЕКТИРУЮЩИХСЯ ИНФОРМАЦИОННЫХ ГРАФОВ

Ю. С. Шуткин (Москва)

Рассматривается задача реализации булевых функций информационными графами [1]. Информационный граф по своей структуре не отличается от контактной схемы, однако все его ребра ориентированы, что дает возможность говорить об обходе информационного графа в определенном направлении, то есть от входа к выходу.

В то время как основной характеристикой контактной схемы является ее размер (или объем), фактически равный числу контактов в схеме, для информационных графов важной характеристикой является их временна́я сложность, то есть среднее время вычисления значения функции при моделировании на компьютере.

Одним из требований к контактным схемам является их способность к самокорректированию, то есть устойчивость к возникновению некоторого фиксированного числа поломок (чаще всего рассматриваются поломки вида замыкания или размыкания контактов схемы). Впервые такая задача была поставлена С. В. Яблонским в 1960 г. в [2].

Задача построения самокорректирующихся контактных схем с тех пор была глубоко изучена. Были предложены методы синтеза, позволяющие строить контактные схемы, исправляющие растущее число ошибок при асимптотическом не увеличении объема схемы [3, 4].

Та же задача может быть рассмотрена и для информационных графов. Предполагается, что при моделировании некоторые элементарные функции могут быть вычислены с ошибкой. Стоит задача построения самокорректирующихся информационных графов.

В данной работе рассмотрен случай возникновения ошибок при моделировании, аналогичных ошибкам в самой схеме, т. е. случай поломки вида замыкания или размыкания контактов.

Получен порядок роста для функции Шеннона сложности реализации булевых функций самокорректирующимися информационными графами.

Постановка задачи и формулировка результатов

Общее определение информационного графа и его функционирования можно найти в [1].

В данной статье нам не нужно будет общее определение, поэтому определим информационный граф следующим образом.

Информационным графом будем называть контактную схему, у которой все ребра имеют ориентацию, причем такую, что в графе нет ориентированных циклов.

Цепью в информационном графе будем называть ориентированную цепь. Проводимость цепи определяется аналогично проводимости для контактных схем в [5].

Говорим, что вершина v_2 достижима из вершины v_1 на наборе α, если существует цепь в графе из вершины v_1 в v_2, проводящая на наборе α.

Функция, реализуемая информационным графом определяется следующим образом. Функция равна 1 на наборе α тогда и только тогда, когда выходной полюс достижим из входного на этом наборе. Видно, что определение согласуется с реализацией функции контактной схемой.

Сложностью (или временно́й сложностью) информационного графа G на наборе α назовем величину

$$T(G,\alpha) = \sum_{v\in\theta(\alpha)} \psi(v),$$

где $\psi(v)$ — количество ребер, выходящих из вершины v, а $\theta(\alpha)$ — множество вершин, достижимых из входного полюса на наборе α.

Сложностью информационного графа назовем величину

$$T(G) = \sum_{\alpha\in\{0,1\}^n} T(G,\alpha)P(\alpha) = E_\alpha\big(T(G,\alpha)\big),$$

где $P(\alpha)$ — вероятность набора α (далее считаем, что имеет место равномерное распределение наборов, т. е. $P(\alpha) = 2^{-n}$ для всех наборов α.)

Считаем, что проводимость некоторого ребра может быть установлена в тождественную 1 (в 0), при этом будем говорить, что в данном ребре произошло *замыкание* (*размыкание*).

Скажем, что информационный граф, реализующий булеву функцию f, *исправляет s размыканий и k замыканий*, если при условии, что графе произошло не более s размыканий и не более k замыканий, он все равно реализует булеву функцию f.

Пусть $U(f,s,k)$ — множество информационных графов, реализующих функцию f и исправляющих s размыканий и k замыканий. *Сложностью функции для s размыканий и k замыканий* назовем величину $T(f,s,k) = \inf\limits_{G \in U(f,s,k)} T(G)$.

Функцию Шеннона сложности определим как

$$T^{Sh}(n,s,k) = \max_{f \in P_2^{(n)}} T(f,s,k).$$

Известно, что при отсутствии ошибок любую б. ф. можно реализовать информационным графом со сложностью не более $2n$ [6].

Теорема. *Для любых $s = s(n)$, $k = k(n)$ функция Шеннона $T^{Sh}(n,s,k)$ по порядку равна nks при $n \to \infty$.*

Автор выражает благодарность Гасанову Э. Э. за постановку задачи и помощь в исследовании.

Список литературы

1. Гасанов Э. Э., Кудрявцев В. Б. Теория хранения и поиска информации. — М.: Физматлит, 2002.

2. Потапов Ю. Г., Яблонский С. В. О синтезе самокорректирующихся контактных схем // ДАН СССР. — 1960. — Т. 134, № 3. — С. 544–547.

3. Редькин Н. П. О самокорректирующихся контактных схемах // Проблемы кибернетики. Вып. 33. — 1978. — С. 119–138.

4. Андреев А. Е. Универсальный принцип самокорректирования // Математический сборник. — 1985. — 127 (169), № 2 (6). — С. 147–172.

5. Лупанов О. Б. Асимптотические оценки сложности управляющих систем. — М.: Изд-во МГУ, 1984.

6. Шуткин Ю. С. О реализации булевых функций информационными графами // Дискретная математика. — 2008. — Т. 20, вып. 4. — С. 31–41.

О СЛОЖНОСТИ ПРОБЛЕМЫ ЭКВИВАЛЕНТНОСТИ АВТОМАТОВ, РАБОТАЮЩИХ НА ЛЕНТАХ РАЗЛИЧНЫХ ТИПОВ

В. Л. Щербина (Москва)

Конечный автомат в ходе вычисления перемещается по линейной ленте в одном направлении. В работе рассматривается обобщение,

допускающее ленты различной структуры и с различными операциями перемещения.

Лентой назовём тройку $\langle S, M, \hat{s}\rangle$, где S — множество ячеек, M — конечное множество отображений типа $S \to S$ (операций перемещения), $\hat{s} \in S$ — начальная ячейка ленты.

Будем считать, что фиксирован конечный алфавит A символов, которые могут быть записаны в ячейках ленты. Содержимое ленты может быть представлено функцией $\xi\colon S \to A$.

Автоматом над лентой $\langle S, M, \hat{s}\rangle$ назовём набор $\langle Q, \hat{q}, \check{q}, \delta, \tau\rangle$, где Q — конечное множество состояний автомата, $\hat{q} \in Q$ — начальное состояние, $\check{q} \notin Q$ — заключительное состояние, $\delta\colon Q \times A \to Q \cup \{\check{q}\}$ — функция перехода, $\tau\colon Q \times A \to M$ — функция перемещения.

Вычислением автомата $\langle Q, \hat{q}, \check{q}, \delta, \tau\rangle$ на ленте $\langle S, M, \hat{s}\rangle$ с содержимым ξ называется конечная или бесконечная последовательность

$$(q_0, s_0), (q_1, s_1), \ldots, (q_n, s_n), \ldots$$

удовлетворяющая следующим условиям:

- $q_i \in Q \cup \{\check{q}\}, s_i \in S$ для $i \geq 0$,
- $q_0 = \hat{q}$, $q_0 = \hat{s}$,
- $q_{i+1} = \delta(q_i, \xi(s_i)), s_{i+1} = \tau(q_i, \xi(s_i))(s_i)$ для $i \geq 0$,
- последовательность заканчивается элементом (q_n, s_n) тогда и только тогда, когда $q_n = \check{q}$.

В случае конечной последовательности *результатом* вычисления считается значение s_n, а в случае бесконечной — особое значение $\perp \notin S$.

Для исследования сложностных аспектов данной модели вычислений была выбрана проблема эквивалентности автоматов.

Два автомата над лентой $\langle S, M, \hat{s}\rangle$ называются *эквивалентными*, если для любого содержимого ленты $\xi\colon S \to A$ результаты их вычислений совпадают.

Пример. Лента $\langle \mathbb{N}, \{\lambda n.n + 1\}, 0\rangle$ приводит к модели, во многом похожей на детерминированные конечные автоматы. Отличия состоят в том, что входом вычисления является не слово, а бесконечная последовательность символов, а результатом — не вердикт "принято/отвергнуто", а ячейка ленты, в которой завершилось вычисление. Проблема эквивалентности автоматов над данной лентой разрешима за полиномиальное время (размером задачи считается количество состояний обоих автоматов).

Автором работы доказаны следующие утверждения.

Теорема. *Пусть* $\langle F_2, \cdot \rangle$ *— свободная группа ранга* 2*, порождённая элементами* a *и* b*, и* ε *— нейтральный элемент этой группы. Проблема эквивалентности автоматов над лентой* $\left\langle F_2, \{\lambda x.x \cdot a, \lambda x.x \cdot a^{-1}, \lambda x.x \cdot b, \lambda x.x \cdot b^{-1}\}, \varepsilon \right\rangle$ *является EXPTIME-полной.*

Теорема. *Проблема эквивалентности автоматов над лентой* $\langle \mathbb{N} \times \mathbb{N}, \{\lambda(x,y).(x+1,y), \lambda(x,y).(x,y+1), \lambda(x,y).(0,0)\}, (0,0)\rangle$ *является PSPACE-полной.*

Теорема. *Пусть* T *— множество всех термов, составленных из константного символа* c *и двухместного функционального символа* f*. Проблема эквивалентности автоматов над лентой*

$$\begin{aligned} \langle\, T \times T, \{&\lambda(x,y).(f(x,y),y),\\ &\lambda(x,y).(x,f(x,y)),\\ &\lambda(x,y).(c,y),\\ &\lambda(x,y).(x,c)\}, (c,c)\,\rangle \end{aligned}$$

является PSPACE-полной.

Теорема. *Проблема эквивалентности автоматов над лентой* $\langle \mathbb{N} \times \mathbb{N}, \{\lambda(x,y).((x+1)\%y, y), \lambda(x,y).(0, y+1)\}, (0,1)\rangle$*, где* $(x+1)\%y$ *— остаток от деления* $x+1$ *на* y*, является NP-полной.*

Список литературы

1. Захаров В. А. Быстрые алгоритмы разрешения эквивалентности операторных программ на уравновешенных шкалах // Математические вопросы кибернетики. Вып. 7. — М.: Физматлит, 1998. — С. 257–280.

2. Ляпунов А. А. О логических схемах программ // Проблемы кибернетики. Вып. 1. — М.: Физматгиз, 1958. — С. 46–74.

3. Подловченко Р. И. Полугрупповые модели программ // Программирование. — 1981. — № 4. — С. 9–19.

4. Янов Ю. И. О логических схемах алгоритмов // Проблемы кибернетики. Вып. 1. — М.: Физматгиз, 1958. — С. 75–127.

Секция «Дискретная геометрия»

ВЫЧИСЛЕНИЕ ВЕКТОРНОГО ПРОИЗВЕДЕНИЯ ТРЕХМЕРНЫХ ВЕКТОРОВ С ИСПОЛЬЗОВАНИЕМ 5 УМНОЖЕНИЙ

А. Я. Белянков (Москва)

В работе [1] Штрассен открыл алгоритм вычисления произведения $N \times N$-матриц A, B асимптотической сложности $O(N^\omega)$, $\omega = \log_2(7) \approx 2.807\ldots$, вместо обычной $O(N^3)$. Алгоритм Штрассена основан на своеобразном способе вычисления набора из четырех билинейных по a, b форм $f_{ij} = (ab)_{ij}$, где a, b суть 2×2-матрицы: экономится одна операция умножения (семь вместо восьми) при значительном "перерасходе" аддитивных операций (примерно полтора десятка вместо четырех). Показатель ω оказался зависящим исключительно от общего количества операций умножения. Этот пример, в котором экономия одной операции умножения имеет решающее значение, делает интересными иные примеры наборов билинейных функций, вычисление которых можно организовать с экономией операций умножения.

Рассмотрим следующий набор из трех билинейных функций f_i от трехмерных векторов a, b (обычное векторное произведение $a \times b$):

$$(f_1, f_2, f_3) = (a^2b^3 - a^3b^2, a^3b^1 - a^1b^3, a^1b^2 - a^2b^1). \tag{1}$$

Общее количество операций умножения равно, очевидно, 6. В [2] показано, что количество умножений при вычислении (1) может быть уменьшено до 5. Другой способ вычисления (1) с 5 умножениями дает

Теорема 1. *Найдутся такие* 15 *трехмерных векторов-столбцов* $\lambda_1, \ldots, \lambda_5$, $\mu_1, \ldots, \mu_5$, $\nu_1, \ldots, \nu_5$ *с элементами из множества* $\{0, \pm 1\}$, *что верно тождество по* a, b *вида*

$$\begin{pmatrix} a^2b^3 - a^3b^2 \\ a^3b^1 - a^1b^3 \\ a^1b^2 - a^2b^1 \end{pmatrix} = \sum_{\rho=1}^{5} \langle \lambda_\rho, a\rangle \, \langle \mu_\rho, b\rangle \, \nu_\rho, \tag{2}$$

где $\langle \bullet, \bullet \rangle$ *– стандартное скалярное произведение.*

Доказательство. Прямая подстановка следующих векторов:

$$(\lambda_1 \mid \mu_1 \mid \nu_1 \mid \ldots \mid \lambda_5 \mid \mu_5 \mid \nu_5) = \begin{pmatrix} + & + & \circ & \circ & \circ & - & + & + & \circ & + & + & \circ & \circ & \circ & + \\ \circ & - & - & \circ & + & + & \circ & - & + & - & \circ & \circ & + & \circ & \circ \\ \circ & + & \circ & + & \circ & - & + & \circ & - & + & \circ & + & \circ & + & \circ \end{pmatrix}, \tag{3}$$

где ради экономии места числа 0, 1, -1 заменены на "$\circ$", "$+$", "$-$".

Скалярным умножением обеих частей на переменный трехмерный вектор c тождество (2) (по a, b) можно эквивалентно преобразовать в следующее тождество по a, b, c:

$$\det(a \mid b \mid c) = \sum_{\rho=1}^{5} \langle \lambda_\rho, a \rangle \langle \mu_\rho, b \rangle \langle \nu_\rho, c \rangle , \tag{4}$$

поскольку $\langle a \times b, c \rangle = \det(a \mid b \mid c)$. По сравнению с обычной формулой для детерминанта порядка 3 правая часть (4) содержит 10 умножений вместо 12. Для иллюстрации выпишем явно тождество (4), соответствующее конкретным векторам $\lambda_\rho, \mu_\rho, \nu_\rho$ из (3):

$$\det(a \mid b \mid c) = (a^1)(b^1 - b^2 + b^3)(-c^2) + (a^3)(b^2)(-c^1 + c^2 - c^3) + \\ +(a^1 + a^3)(b^1 - b^2)(c^2 - c^3) + (a^1 - a^2 + a^3)(b^1)(c^3) + (a^2)(b^3)(c^1).$$

Правая часть (4) не изменится, если переставить слагаемые, а также если в некоторых слагаемых поменять знаки у каких-то двух из $\lambda_\rho, \mu_\rho, \nu_\rho$. Если две формулы вида (4) переводятся друг в друга указанными преобразованиями, то считаем, что это одна и та же формула. Тогда число разных формул вида (4) равно 96.

Была рассмотрена также аналогичная детерминанту трилинейная форма, — так называемый перманент порядка 3:

$$\operatorname{perm}(a \mid b \mid c) = a^1 b^2 c^3 + a^2 b^3 c^1 + a^3 b^1 c^2 + a^2 b^1 c^3 + a^1 b^3 c^2 + a^3 b^2 c^1.$$

Теорема 2. *Найдутся такие* 15 *трехмерных векторов-столбцов* $\lambda_1, \ldots, \lambda_5$, $\mu_1, \ldots, \mu_5$, $\nu_1, \ldots, \nu_5$ *с элементами из множества* $\{0, \pm 1\}$, *что верно тождество по* a, b, c *вида*

$$\operatorname{perm}(a \mid b \mid c) = \sum_{\rho=1}^{5} \langle \lambda_\rho, a \rangle \langle \mu_\rho, b \rangle \langle \nu_\rho, c \rangle . \tag{5}$$

Доказательство. Прямая подстановка следующих векторов:

$$(\lambda_1 \mid \mu_1 \mid \nu_1 \mid \ldots \mid \lambda_5 \mid \mu_5 \mid \nu_5) =$$
$$\begin{pmatrix} + & + & \circ & \circ & \circ & + & + & + & \circ & + & + & \circ & \circ & \circ & + \\ \circ & - & - & \circ & + & + & \circ & - & + & + & \circ & \circ & + & \circ & \circ \\ \circ & - & \circ & + & \circ & - & + & \circ & - & + & \circ & + & \circ & + & \circ \end{pmatrix}. \tag{6}$$

Число разных формул вида (5) равно 168.

Результаты были получены путем такого же, как в [3, 4], полного компьютерного перебора с использованием описанного там приема разделения построения тождества с коэффициентами из множества $\{0, \pm 1\}$ на два этапа: 1) после редуцирования исходной задачи в более простую аналогичную алгебраическую задачу над полем Z_2 путем применения операции $\bmod 2$ к обеим частям равенства и последующего решения редуцированной задачи интерпретируем полученное решение как носитель решения исходной задачи; 2) решаем задачу расстановки знаков в решении-носителе, состоящую в замене каждого элемента $1 \in Z_2$ на целые числа 1 или -1 так, чтобы получилось решение исходной задачи.

Эти результаты делают более правдоподобным существование тождеств штрассеновского типа с коэффициентами из $\{0, \pm 1\}$, для поиска которых можно использовать прием из предыдущего абзаца.

Список литературы

1. Strassen V. Gaussian elimination is not optimal // Numer. Math. — 1969. — V. 13, № 4. — P. 354–356.

2. Fiduccia C. M. On the algebraic complexity of matrix multiplication. PhD Thesis, Brown Univ., 1973.

3. Белянков А. Я. Перебор всех штрассеновских алгоритмов для (2x2)-матриц // Материалы IX Международного семинара "Дискретная математика и ее приложения", посвященного 75-летию академика О. Б. Лупанова (18–23 июня 2007 г.). — М.: Изд-во механико-математического факультета МГУ, 2007. — С. 366–369.

4. Белянков А. Я. Вычисление коммутатора 2x2-матриц с использованием 5 умножений // Журнал вычислительной математики и математической физики. — 2008. — Т. 48, вып. 2. — С. 201–205.

НОВЫЕ ОЦЕНКИ В ЗАДАЧЕ ДАНЦЕРА — ГРЮНБАУМА ОБ ОСТРОУГОЛЬНЫХ ТРЕУГОЛЬНИКАХ

Л. В. Бучок (Москва)

Данная работа посвящена оценкам мощностей множеств точек евклидова пространства, в которых никакие три точки не образуют прямого или тупого угла. Введём обозначения: $a(n)$ — мощность максимального множества $S \subseteq \mathbb{R}^n$, обладающего указанным свойством; $k(n)$ — мощность максимального множества $S \subseteq \{0,1\}^n$, обладающего тем же свойством. Очевидно, $k(n) \leq a(n)$. Кроме того, известно, что $a(n) \leq 2^n$.

В 1962 году Л. Данцер и Б. Грюнбаум высказали гипотезу [1] о том, что $a(n) = 2n - 1$. В 1983 году эта гипотеза была опровергнута П. Эрдешем и З. Фюреди [2], доказавшими с помощью вероятностного метода, что $k(n) \geq \left\lfloor \frac{1}{2}\left(\frac{2}{\sqrt{3}}\right)^n \right\rfloor$. В 2006 году Д. Беван путём изменения параметров в методе Эрдеша—Фюреди показал [3], что

$$k(n) \geq 2\left\lfloor \frac{\sqrt{6}}{9}\left(\frac{2}{\sqrt{3}}\right)^n \right\rfloor = 0.544\cdots \times (1.154\ldots)^n.$$

Также Д. Беван получил оценку

$$a(n) \geq 2\left\lfloor \frac{1}{3}\left(\frac{2}{\sqrt{3}}\right)^{n+1} \right\rfloor = 0.770\cdots \times (1.154\ldots)^n$$

и ряд результатов для малых размерностей n, вследствие чего гипотеза Данцера—Грюнбаума была опровергнута при $n \geq 7$. Отметим, что при $n \leq 3$ гипотеза справедлива, и неясность сохраняется лишь при $n = 4, 5, 6$. Также, существует оценка

$$a(n) \geq C\sqrt{n}\left(\frac{2}{\sqrt{3}}\right)^n,$$

полученная Э. Акерманом и О. Бен-Цви в 2008 году [4]. Точное значение константы C для этой оценки неизвестно.

Теорема 1 (Эрдеш, Фюреди, 1983). *Имеет место неравенство*

$$k(n) \geq \left\lfloor \frac{1}{2}\left(\frac{2}{\sqrt{3}}\right)^n \right\rfloor.$$

Схема доказательства. Положим $m = \left\lfloor \frac{1}{2}\left(\frac{2}{\sqrt{3}}\right)^n \right\rfloor$ и возьмём случайное (мульти)множество $S \subseteq \{0,1\}^n$ из $2m$ (не обязательно различных) $(0,1)$-векторов; при этом координаты каждого вектора $\vec{v} = (v_1, v_2, ..., v_n) \in S$ мы выберем независимо, с вероятностью

$$P(v_i = 0) = P(v_i = 1) = \frac{1}{2}, 1 \le i \le n;$$

выбор самих векторов мы также осуществим независимо.

Назовём тройку векторов $(\vec{u}, \vec{v}, \vec{w}) \subset S$ *обобщённым прямым углом* с вершиной в $\vec{w}$, если $(\vec{u} - \vec{w}, \vec{v} - \vec{w}) = 0$. Заметим, что все прямые углы в нашем множестве являются обобщёнными прямыми углами, а отрицательных значений упомянутое скалярное произведение принимать не может. Тройка $(\vec{u}, \vec{v}, \vec{w})$ является обобщённым прямым углом с вершиной в $\vec{w}$ тогда и только тогда, когда набор (u_i, v_i, w_i) не имеет вид $(0,0,1)$ или $(1,1,0)$ ни для какого $i \in \{1, \ldots, n\}$. Вероятность последнего события равна $\left(\frac{3}{4}\right)^n$. Значит, математическое ожидание количества обобщённых прямых углов в S равно $3C_{2m}^3 \left(\frac{3}{4}\right)^n$. Поскольку $3C_{2m}^3 \left(\frac{3}{4}\right)^n \le m$ в силу выбора m, найдётся множество S из $2m$ векторов, в котором не более m обобщённых прямых углов. Если мы удалим из S вершины всех этих углов, останется множество из не менее m различных точек, никакие три из которых не образуют прямой угол. Таким образом, $k(n) \ge m$, и схема доказательства теоремы завершена.

Автором данной работы было разработано несколько новых подходов к решению задачи на основе метода Эрдеша–Фюреди, в результате чего были последовательно получены следующие новые оценки для $k(n)$ и $a(n)$.

Теорема 2 [5]. *Имеют место неравенства*

$$k(n) \ge \frac{3}{2}\left\lfloor \frac{11\sqrt{66}}{243}\left(\frac{2}{\sqrt{3}}\right)^n \right\rfloor = 0.551\cdots \times (1.154\ldots)^n,$$

$$a(n) \ge \frac{3}{2}\left\lfloor \frac{22\sqrt{33}}{243}\left(\frac{2}{\sqrt{3}}\right)^n \right\rfloor = 0.780\cdots \times (1.154\ldots)^n.$$

Теорема 3. *Имеет место неравенство*

$$a(n) \ge \frac{2}{3}\left\lfloor \sqrt{2}\left(\frac{2}{\sqrt{3}}\right)^n \right\rfloor \approx 0.9428\ldots \times (1.154\ldots)^n.$$

Теорема 4. *Имеет место неравенство*

$$k(n) \geq \left\lfloor \frac{2}{3}\left(\frac{2}{\sqrt{3}}\right)^n \right\rfloor \approx 0.666\ldots \times (1.154\ldots)^n.$$

Работа выполнена при финансовой поддержке гранта РФФИ № 09-01-00294.

Список литературы

1. Danzer L., Grünbaum B. Über zwei Probleme bezüglich konvexer Körper von P. Erdős und von V. L. Klee // Math. Zeitschrift. — 1962. — V. 79. — P. 95–99.

2. Erdős P.,Füredi Z. The greatest angle among n points in the d-dimensional Euclidean space // Annals of Discrete Math. — 1983. — V. 17. — P. 275–283.

3. Bevan D. Sets of points determining only acute angles and some related colouring problems // The Electronic Journal of Combinatorics. — 2006. — V. 13. — № R12.

4. Ackerman E., Ben-Zwi O. On sets of points that determine only acute angles // European Journal of Combinatorics. — 2008. — V. 30, I. 4. — P. 908–910.

5. Бучок Л. В. Остроугольные треугольники Данцера—Грюнбаума // Успехи математических наук. — 2009. — Т. 64, вып. 3 (387). — С. 181–182.

ПАРАЛЛЕЛОЭДРЫ: ГИПОТЕЗА ВОРОНОГО

А. А. Гаврилюк (Москва)

Понятие параллелоэдра было введено кристаллографом Е. С. Фёдоровым (1885) как одно из основных понятий кристаллографии. *Параллелоэдр* d измерений определяется как выпуклый евклидов многогранник, который своими параллельными копиями разбивает пространство $\mathbb{E}^d$ нормальным образом, т. е. если пересечение двух многогранников не пусто, то оно есть их общая целая грань некоторой размерности. Г. Минковский доказал теорему, дающую необходимые условия того, что многогранник является параллелоэдром. Б. А. Венков показал, что условия Минковского являются достаточными. Позднее МакМюллен независимо переоткрыл теорему Венкова. Н. П. Долбилин доказал *теорему о продолжении*, а также выделил у параллелоэдров так называемые "стандартные

грани", что позволило улучшить доказательства теорем Венкова и Минковского. Г. Ф. Вороной построил теорию специального класса параллелоэдров, в настоящее время называемых *параллелоэдрами Вороного*. Он высказал гипотезу о том, что любой параллелоэдр аффинно-эквивалентен некоторому параллелоэдру Вороного и доказал следующую теорему:

Теорема (Вороной). *Всякий примитивный параллелоэдр аффинно-эквивалентен некоторому параллелоэдру Вороного.*

О. К. Житомирский усилил теорему Вороного, доказав гипотезу для $(d-2)$-примитивных параллелоэдров (это условие эквивалентно тому, что в каждой $(d-2)$-мерной грани сходятся ровно 3 параллелоэдра). Эрдал доказал гипотезу Вороного для параллелоэдров, которые являются зоноэдрами. Напомним, что зоноэдр — это многогранник, являющийся суммой Минковского конечного количества отрезков. А. Ордин доказал гипотезу в случае, так называемых, 3-*неразложимых* параллелоэдров.

Напомним основную идею Вороного доказательства его теоремы. Пусть дано разбиение T пространства $\mathbb{E}^d$ параллельными копиями данного параллелоэдра P. Пусть K_{d-1} — множество гиперграней этого комплекса. Для некоторых параллелоэдров P удаётся построить так называемую *каноническую нормировку* — отображение $S : K_{d-1} \to \mathbb{R}_+$, обладающее рядом свойств (см. [6, 8]). В случае, если каноническая нормировка существует, можно показать существование кусочно-линейной функции $G : \mathbb{E}^d \to \mathbb{R}_+$, которая является линейной на ячейках T. Вороной ввёл эту функцию для примитивных параллелоэдров и назвал её женератрисой. Её график описан около эллиптического параболоида $x_{n+1} = Q(x_1, x_2, \ldots, x_n)$, где Q — положительно определённая квадратичная форма. По этой квадратичной форме строится аффинное преобразование, переводящее данный параллелоэдр P в некоторый параллелоэдр Вороного. Верна следующая теорема:

Теорема. *Пусть задан некоторый примитивный d-параллелоэдр P и разбиение T пространства $\mathbb{E}^d$ на параллельные копии P. Тогда существует каноническая нормировка комплекса* T.

Прямое приложение данной теоремы приводит нас к доказательству теоремы Вороного.

Вершину параллелоэдра назовём *почти примитивной*, если все смежные с ней вершины данного параллелоэдра лежат в одной $(d-1)$-мерной гиперплоскости. Параллелоэдр назовём *почти примитивным*, если все его вершины почти примитивны.

Теорема (о почти примитивных параллелоэдрах). *Всякий почти примитивный параллелоэдр аффинно-эквивалентен некоторому па-*

раллелоэдру Вороного.

Нам потребуется ещё одно определение. Пусть в $\mathbb{E}^d$ задан многогранник P и начало координат принадлежит этому многограннику. Тогда *полярным* к P многогранником называется $P^\Delta = \{c \in \mathbb{E}^d | cx \leqslant 1 \text{ для всех } x \in P\}$. Пусть Q — выпуклая оболочка одномерного остова звезды $star(v)$ некоторой вершины v комплекса T. Тогда граням из $star(v)$ размерности k этого комплекса будут соответствовать грани размерности $(k-1)$ многогранника Q. При взятии полярного многогранника l-граням Q соответствуют $(d-1-l)$-грани Q^Δ. Выполнив последовательно эти два отображения, получим, что $(d-1)$-мерным граням из $star(v)$ соответствуют одномерные рёбра Q^Δ. Оказывается, что положив нормирующие коэффициенты равными длинам этих одномерных рёбер, мы получим (локальную) каноническую нормировку для $star(v)$. Отметим, что *примитивный* параллелоэдр является частным случаем *почти примитивного*. То есть данная теорема является усилением теоремы Вороного. Сравнивая этот результат с теоремой Житомирского, обнаруживается, что описываемые ими случаи пересекаются, но не покрывают друг друга. Например, прямое произведение отрезка на почти примитивный параллелоэдр является почти примитивным, но не является $(d-2)$-примитивным. С другой стороны, уже в размерности 3 есть параллелоэдры $(d-2)$-примитивные, но не являющиеся почти примитивными (комбинаторно эквивалентны ромбододекаэдру).

Автор выражает глубокую благодарность Николаю Петровичу Долбилину за знакомство с замечательной темой параллелоэдров и постановку задачи, Алексею Игоревичу Гарберу, за продуктивное обсуждение и терпеливое выслушивание не самого структурированного математического текста.

Список литературы

1. Minkowski H. Allgemeine Leherzätze über konvexe Polyeder // Nach. Ges. Wiss. — Göttingen, 1897. — P. 198-219.

2. Венков Б. А. Об одном классе эвклидовых многогранников // Вестник Ленинградского Университета. Сер. Мат., физ., хим. — 1954. — Т. 9. — С. 11–31.

3. Dolbilin N. P. The extension theorem // Discrete mathematics. — 2000. — Т. 221, № 1–3. — P. 43–60.

4. Долбилин Н. П., Макаров В. С. Теорема о продолжении в теории правильных разбиений и ее приложения // Труды МИАН. — 2002. — Т. 239. — С. 136–159.

5. Долбилин Н. П. Свойства граней параллелоэдров // Труды МИАН. — 2009. — Т. 266. — С. 112–126.

6. Voronoy G. Nouvelles applications des paramétres continus á la theorie des formes quadratiques // II Mémoire: Recherches sur les parallélоédres primitifss. — 1909. — Crelle Journ. — № 134. — P. 67-178; (Собрание сочинений, т. II. — 1952).

7. Erdahl R. Zonotopes, dicings, and Voronoi's conjecture on parallelohedra // Eur. J. Comb. — 1999. — V. 20 (6). — P. 527–549.

8. Ordine A. Proof of the Voronoy conjecture on parallelotopes in a new special case // Queen's University, Kingston, 2005.

О КЛАССАХ ТРИАНГУЛЯЦИЙ ТОЧЕЧНЫХ КОНФИГУРАЦИЙ

Д. В. Груздев (Нижний Новгород)

В развитие [1] рассматривается пять классов триангуляций точечных конфигураций (в т. ч. классы слаборегулярных [2], разворачиваемых, симплициально политопиальных триангуляций [1]), по отношению принадлежности/непринадлежности к которым множество всех триангуляций точечных конфигураций разбивается на 32 попарно непересекающихся подкласса. Установлено, что из данных 32 подклассов в точности 20 подклассов являются непустыми, и для каждого из 20 непустых подклассов показано, что множество комбинаторных типов его триангуляций является счётным.

Рассмотрим d-мерный выпуклый многогранник $M \subset \mathrm{R}^d$, который будем называть также *d-мерным политопом*, и обозначим через $\Gamma_i(M)$ множество его i-мерных граней, $i = -1, \ldots, d$. При этом $\Gamma_{-1}(M) = \{\emptyset\}$ и $\Gamma_d(M) = \{M\}$. Положим $\dim(M) = d$, $\Gamma(M) = \bigcup_{i=-1}^{d} \Gamma_i(M)$ и $\Gamma^{\partial}(M) = \bigcup_{i=-1}^{d-1} \Gamma_i(M)$. Через $\partial(M)$ обозначим границу политопа M. Если $|\Gamma_0(M)| = d+1$, то политоп M называется *d-мерным симплексом*. Политоп M называется *симплициальным*, если все его $(d-1)$-мерные грани являются $(d-1)$-мерными симплексами. Выпуклую оболочку множества точек A' обозначим через $[A']$.

Конечное множество точек $A = \{a_1, \ldots, a_n\} \subset \mathrm{R}^d$, выпуклая оболочка $[A]$ которого есть d-мерный политоп, называется *d-мерной точечной конфигурацией*. *Триангуляцией* d-мерной точечной конфигурации A называется такое множество $T = \{S_1, \ldots, S_t\}$ d-мерных

симплексов $S_1, \ldots, S_t$ с вершинами из A, что их объединение есть политоп $[A]$ и пересечение любых двух симплексов из T является их общей гранью (возможно, пустой). Политоп $M(T) = \bigcup_{j=1}^{t} S_j = [A]$ назовём *многогранником триангуляции* T. Положим $\Gamma(T) = \bigcup_{j=1}^{t} \Gamma(S_j)$ и $\Gamma^{\partial}(T) = \{F \in \Gamma(T) \ : \ F \subset \partial([A])\}$, $\Gamma_i(T) = \bigcup_{j=1}^{t} \Gamma_i(S_j)$, $\Gamma_i^{\partial}(T) = \{F \in \Gamma_i(T) \ : \ F \in \Gamma^{\partial}(T)\}$, $\Gamma_i^{int}(T) = \Gamma_i(T) \backslash \Gamma_i^{\partial}(T)$ при $i = -1, \ldots, d$. Через $\mathcal{T}'_d$ обозначим множество триангуляций d-мерных точечных конфигураций и положим $\mathcal{T}' = \bigcup_{d=0}^{+\infty} \mathcal{T}'_d$.

Симплициальные комплексы называются *изоморфными*, если между ними можно установить биекцию, сохраняющую отношение включения. Триангуляция $T \in \mathcal{T}'$ называется *слаборегулярной* (weakly regular) [2], если существует такая регулярная (regular, правильная, см., например, [2]) триангуляция $T' \in \mathcal{T}'$, что симплициальные комплексы $\Gamma(T)$ и $\Gamma(T')$ изоморфны.

Триангуляция T называется *разворачиваемой* (shellable), если существует такая последовательность ее симплексов $(S_1, \ldots, S_t)$, что $T = \{S_1, \ldots, S_t\}$ и при $l = 2, \ldots, t$ множество $\Gamma(S_l) \backslash \bigcup_{i=1}^{l-1} \Gamma(S_i)$ имеет единственный минимальный по включению элемент.

Триангуляцию $T \in \mathcal{T}'$ назовём *симплициально политопиальной* [1], если для неё существует такой симплициальный политоп P, что симплициальные комплексы $\Gamma^{\partial}(T)$ и $\Gamma^{\partial}(P)$ изоморфны.

Через $\mathcal{T}^{WR}$, $\mathcal{T}^{Sh}$ и $\mathcal{T}^{SP}$ обозначим соответственно множества слаборегулярных, разворачиваемых и симплициально политопиальных триангуляций из $\mathcal{T}'$. Положим $\mathcal{T}^{int} = \{T \in \mathcal{T}' : \Gamma_0^{int}(T) \neq \emptyset\}$ и $\mathcal{T}'^{\partial} = \{T \in \mathcal{T}' : \Gamma_0^{\partial}(T) \backslash \Gamma_0(M(T)) \neq \emptyset\}$. Таким образом, исследуются пять классов триангуляций: $\mathcal{T}^{WR}$, $\mathcal{T}^{Sh}$, $\mathcal{T}^{SP}$, $\mathcal{T}^{int}$ и $\mathcal{T}'^{\partial}$. При $\mathcal{T} \subseteq \mathcal{T}'$ положим $\mathcal{T}^0 = \mathcal{T}' \backslash \mathcal{T}$ и $\mathcal{T}^1 = \mathcal{T}$. Тогда $\mathcal{T}'$ разбивается на 32 попарно непересекающихся подкласса $\mathcal{T}_{i_1,i_2,i_3,i_4,i_5} = (\mathcal{T}^{WR})^{i_1} \cap (\mathcal{T}^{Sh})^{i_2} \cap (\mathcal{T}^{SP})^{i_3} \cap (\mathcal{T}^{int})^{i_4} \cap (\mathcal{T}'^{\partial})^{i_5}$, где $i_1, \ldots, i_5 \in \{0, 1\}$.

Для $T \in \mathcal{T}'_d$ положим $s(T) = |\Gamma_{d-1}^{\partial}(T) \cap \Gamma_{d-1}(M(T))|$.

Положим $T_0 = \{[(0,0),(0,1),(1,0)]\}$ и заметим, что $T_0 \in \mathcal{T}_{1,1,1,0,0}$ и $s(T) = 3$. Известно [2], что $\mathcal{T}^{WR} \subset \mathcal{T}^{Sh}$. В [2] построена триангуляция из $\mathcal{T}_{0,1,1,0,0}$, которую обозначим через T_1, а из [3] следует существование триангуляции из $\mathcal{T}_{0,0,1,0,0}$, обозначаемой здесь через T_2 и являющейся модификацией известного примера M.E. Rudin триангуляции из $\mathcal{T}_{0,0,1,0,1}$, причём $s(T_1) = 10$, $s(T_2) = 24$, $T_i \in \mathcal{T}'_3$ и $\Gamma_2^{\partial}(T) = \Gamma_2(M(T_i))$ при $i = 1, 2$. Таким образом, $\mathcal{T}^{WR} \subset \mathcal{T}^{Sh} \subset \mathcal{T}'$.

Лемма 1. $\mathcal{T}^{WR} \subset \mathcal{T}^{Sh} \cap \mathcal{T}^{SP}$.

Для $w = (w_1, \ldots, w_d) \in \mathrm{R}^d$ положим $\psi(w) = (w_1, \ldots, w_d, 0) \in \mathrm{R}^{d+1}$, а для $M \subset \mathrm{R}^d$ положим $\psi(M) = \{\psi(w) : w \in M\}$. Для триангуляции $T \in \mathcal{T}'_d$ положим $\eta(T) = \{[\psi(S), e_{d+1}] : S \in T\}$, где $e_{d+1} = (0, \ldots, 0, 1) \in \mathrm{R}^{d+1}$, и заметим, что $\eta(T) \in \mathcal{T}'_{d+1}$.

Лемма 2. *Если* $i_2, \ldots, i_5 \in \{0,1\}$ *и* $T \in \mathcal{T}_{0,i_2,i_3,i_4,i_5}$, *то* $\eta(T) \in \mathcal{T}_{0,i_2,0,0,\max\{i_4,i_5\}}$ *и* $s(\eta(T)) \geq s(T)$.

Лемма 3. *Если* $i_2, \ldots, i_5 \in \{0,1\}$ *и* $T \in \mathcal{T}_{1,i_2,i_3,i_4,i_5}$, *то* $i_2 = 1$, $i_3 = 1$, $\eta(T) \in \mathcal{T}_{1,1,1,0,\max\{i_4,i_5\}}$ *и* $s(\eta(T)) \geq s(T)$.

Теперь рассмотрим такую триангуляцию $T \in \mathcal{T}'$, что $s(T) \geq 1$ и $d = \dim(M(T)) \geq 2$. Тогда существуют такие точки $v_0, v_1, \ldots, v_d \in \mathrm{R}^d$, что грань $F = [v_1, \ldots, v_d] \in \Gamma^{\partial}_{d-1}(T) \cap \Gamma_{d-1}(M(T))$ и точка v_0 расположена над F и под всеми остальными (d-1)-мерными гранями политопа $M(T)$ и не принадлежит аффинной оболочке ни одной (d-1)-мерной грани политопа $M(T)$. Пусть $p_1 = \frac{1}{d+1}\sum_{k=0}^{d} v_k$, $p_2 = \frac{1}{d}\sum_{k=0}^{d-1} v_k$, $T_{0,0} = \{[v_0, \ldots, v_d]\}$, $T_{0,1} = \{[\{v_0, \ldots, v_d, p_2\}\backslash\{v_k\}] : k = 0, \ldots, d-1\}$, $T_{1,0} = \{[\{p_1, v_0, \ldots, v_d\}\backslash\{v_k\}] : k = 0, \ldots, d\}$, $T_{1,1} = \{[\{p_1, v_0, \ldots, v_d\}\backslash\{v_k\}] : k = 0, \ldots, d-1\} \cup \{[\{p_1, v_0, \ldots, v_{d-1}, p_2\}\backslash\{v_k\}] : k = 0, \ldots, d-1\}$. Положим $\mu_{i_4,i_5}(T) = T \cup T_{i_4,i_5}$ при $i_4, i_5 \in \{0,1\}$. Также положим $\mu^0_{i_4,i_5}(T) = T$ и $\mu^j_{i_4,i_5}(T) = \mu_{i_4,i_5}(\mu^{j-1}_{i_4,i_5}(T))$ при $i_4, i_5 \in \{0,1\}$ и натуральном j .

Лемма 4. *Если* $i_1, \ldots, i_5, k_4, k_5 \in \{0,1\}$, $T \in \mathcal{T}_{i_1,i_2,i_3,k_4,k_5}$, $\dim(M(T)) \geq 2$ *и* $s(T) \geq 1$, *то* $\mu_{i_4,i_5}(T) \in \mathcal{T}_{i_1,i_2,i_3,\max\{i_4,k_4\},\max\{i_5,k_5\}}$ *и* $s(\mu_{i_4,i_5}(T)) \geq s(T)$.

Теорема 1. *Для* $i_4, i_5 \in \{0,1\}$ *и целого неотрицательного* j *выполняются следующие соотношения:*

$\mu_{i_4,i_5}(\mu^j_{0,0}(\eta(T_2))) \in \mathcal{T}_{0,0,0,i_4,i_5}$, $\mu_{i_4,i_5}(\mu^j_{0,0}(T_2)) \in \mathcal{T}_{0,0,1,i_4,i_5}$,

$\mu_{i_4,i_5}(\mu^j_{0,0}(\eta(T_1))) \in \mathcal{T}_{0,1,0,i_4,i_5}$, $\mu_{i_4,i_5}(\mu^j_{0,0}(T_1)) \in \mathcal{T}_{0,1,1,i_4,i_5}$,

$\mathcal{T}_{1,0,0,i_4,i_5} = \emptyset$, $\mathcal{T}_{1,0,1,i_4,i_5} = \emptyset$,

$\mathcal{T}_{1,1,0,i_4,i_5} = \emptyset$, $\mu_{i_4,i_5}(\mu^j_{0,0}(T_0)) \in \mathcal{T}_{1,1,1,i_4,i_5}$.

Теорема 2. *Для каждого из* 20 *подклассов* ($\mathcal{T}_{0,i_2,i_3,i_4,i_5}$, $\mathcal{T}_{1,1,1,i_4,i_5}$, *где* $i_2, \ldots, i_5 \in \{0,1\}$), *множество комбинаторных типов триангуляций данного подкласса является счётным.*

Работа выполнена при поддержке РФФИ, проект 09-01-00545-а.

Список литературы

1. Груздев Д. В. О симплициально политопиальных триангуляци-

ях // IV Всероссийская конференция "Проблемы оптимизации и экономические приложения": Материалы конференции (Омск, 29 июня – 4 июля 2009). — Омск: Полиграфический центр КАН, 2009. — С. 177.

2. Lee C. W. Regular triangulations of convex polytopes // DIMACS Series in Discrete Mathematics and Theoretical Computer Science. — 1991. — V. 4. — P. 443–456.

3. Connelly R., Henderson D. W. A convex 3-complex not simplicially isomorphic to a strictly convex complex // Math. Proc. Camb. Phil. Soc. — 1980. — V. 88. — P. 299–306.

ВСЕ БЕЗ ИСКЛЮЧЕНИЯ РАСКРАСКИ ДЕЙСТВИТЕЛЬНОЙ ПРЯМОЙ, УДОВЛЕТВОРЯЮЩИЕ УСЛОВИЮ ЗАДАЧИ О ХРОМАТИЧЕСКОМ ЧИСЛЕ

М. О. Джексенбаева (Москва)

Задача о хроматическом числе n-мерного евклидова пространства (в классическом варианте) заключается в нахождении минимального количества цветов, в которое можно раскрасить каждую точку пространства так, чтобы расстояние между двумя одинаково окрашенными точками нигде не равнялось 1. На сегодняшний день точное значение хроматического числа известно только для одномерного случая — прямой $\mathbf{R}^1$, и его значение равняется 2. Для доказательства этого факта в [1] используется пример "хорошей" или "правильной" раскраски прямой в два цвета. Она представляет собой чередование через один раскрашенных в первый и второй цвета полуотрезков длины 1.

В общем случае, возьмём на действительной прямой любой полуотрезок длины 1, пусть, для определённости, это будет $[0, 1)$. Раскрасим его произвольным образом в два цвета без пропусков и перекрытий, что всегда допустимо, поскольку расстояние между любыми точками единичного полуотрезка строго меньше 1. Затем перейдём к соседнему полуотрезку $[1, 2)$. Раскрасим его в те же цвета, но "с точностью до наоборот": если точка отстоящая от начала первого полуотрезка на некоторое расстояние, окрашена в один цвет, то точку, отстоящую на такое же расстояние от начала второго полуотрезка, окрасим в противоположный цвет.

Далее будем раскрашивать полуотрезки длины 1 как вправо, так и влево от начального, чередуя "позитивную" и "негативную" раскраску первоначального полуотрезка через один. Полученная раскраска действительной прямой является периодичной с периодом, равным 2, т. е. точка, отстоящая от любой данной на расстояние 2, окрашена в тот же цвет. Описанным способом получаются все без исключения правильные раскраски действительной прямой в два цвета.

Утверждение. *Все раскраски прямой в два цвета, удовлетворяющие условию задачи о хроматическом числе, периодичны с периодом* 2*, причём полупериоды раскрашены противоположно; иначе говоря, раскраски единичных полуотрезков меняются на противоположные через один.*

Нетрудно проверить, что для любой правильной раскраски действительной прямой в два цвета часть прямой, окрашенная в один цвет, и часть, окрашенная в другой, конгруэнтны: для их совмещения достаточно одну из них сдвинуть вдоль прямой на 1.

Автор выражает благодарность Л. М. Коганову за полезные замечания.

Список литературы

1. Райгородский А. М. Хроматические числа. — М.: МЦНМО, 2003.

2. Райгородский А. М. Проблема Борсука и хроматические числа пространств // Материалы VIII Международного семинара "Дискретная математика и её приложения" (2–6 февраля 2004 г.). — М.: Изд-во механико-математического факультета МГУ, 2004. — С. 43–49.

ГЕОМЕТРИЧЕСКИЙ ВЫВОД ФОРМУЛЫ ДЛЯ ЧИСЛА СОБСТВЕННЫХ ВОЛН В ПЛАНАРНОМ ВОЛНОВОДЕ

М. Д. Ковалёв (Москва)

Плоский волновод представляет собой совокупность из $m+1$ слоёв диэлектриков с показателями преломления n_j. Далее будем считать, что в крайних слоях бесконечной толщины $n_1 \geq n_{m+1}$. А среди внутренних слоёв, имеющих толщины $t_2, t_3, \ldots, t_m$, наибольший показатель преломления для волн рассматриваемой частоты $n_k > n_1$

имеется в k-ом слое. Электромагнитные волны, распространяющиеся в волноводе, бывают двух типов: так называемые TE- и TM-волны [1]. Хотя наш подход применим и для TM-волн, мы ради определённости будем говорить лишь о TE-волнах. Если считать слои перпендикулярными оси Ox, а волны распространяющимися вдоль оси Oz, то уравнение в j-м слое для TE-волн записывается в безразмерных переменных так

$$\frac{d^2E_y}{d\xi^2} + \eta_j^2 E_y = \sigma^2 E_y,$$

здесь $E_y(x)$ — составляющая вектора электрической напряжённости поля волны, $\eta_j = \frac{n_j}{n_1}$ — приведённый показатель преломления, могущий быть меньшим единицы (скажем, $\eta_{m+1} \leq 1$), а $\sigma = \frac{\beta}{n_1}$ — приведённый эффективный показатель преломления (β — постоянная распространения).

Хорошо известные в каждом слое решения этого дифференциального уравнения сшиваются на граничных плоскостях слоёв по условиям непрерывности величин E_y и $\frac{dE_y}{dx}$. Если при некотором значении σ получается решение, у которого в крайних бесконечных слоях поле экспоненциально убывает на бесконечности (краевые условия), то это значение приведённого эффективного показателя преломления σ называется собственным, а соответствующее решение — собственной TE-модой или волной волновода. Число TE-мод в волноводе, состоящем из конечного числа слоёв, конечно. Определение его — одна из основных задач теории волноводов.

Автором была предложена новая форма уравнения для определения собственных значений величины σ, которую он назвал многослойным уравнением [2]. На основе этого уравнения были посчитаны [3] числа собственных электромагнитных мод в плоских волноводах из двух материалов. Здесь этот результат усилен и упрощён путём сведения задачи к подсчёту поворота некоторых векторов в плоскости. Исходя из многослойного уравнения, задача нахождения числа собственных TE-волн сводится к подсчёту числа корней уравнения

$$(\vec{a}_{m+1}(\sigma), \vec{A}_m^o(\sigma)) = 0,$$

на интервале $1 < \sigma < \alpha = \frac{n_k}{n_1}$. Здесь вектор функция $\vec{A}_m^o(\sigma) = (\sqrt{\alpha^2 - \sigma^2}, \sqrt{\eta_{m+1}^2 - \sigma^2})$. А вектор функция $\vec{a}_{m+1}(\sigma)$ строится последовательно: $\vec{a}_2(\sigma) = (\sqrt{\sigma^2 - 1}, \sqrt{\alpha^2 - \sigma^2})$, и

$$\vec{a}_{j+1}(\sigma) = V_j(\sigma)\vec{a}_j(\sigma).$$

Здесь матрица непрерывного семейства $V_j(\sigma)$ линейных преобразований имеет следующий вид:

$$\begin{pmatrix} \operatorname{ch} t_j\sqrt{\sigma^2-\eta_j^2} & \frac{\sqrt{\sigma^2-\eta_j^2}}{\sqrt{\alpha^2-\sigma^2}}\operatorname{sh} t_j\sqrt{\sigma^2-\eta_j^2} \\ \frac{\sqrt{\alpha^2-\sigma^2}}{\sqrt{\sigma^2-\eta_j^2}}\operatorname{sh} t_j\sqrt{\sigma^2-\eta_j^2} & \operatorname{ch} t_j\sqrt{\sigma^2-\eta_j^2} \end{pmatrix},$$

при $\eta_j < \sigma < \alpha$,

$$\begin{pmatrix} \cos t_j\sqrt{\eta_j^2-\sigma^2} & -\frac{\sqrt{\eta_j^2-\sigma^2}}{\sqrt{\alpha^2-\sigma^2}}\sin t_j\sqrt{\eta_j^2-\sigma^2} \\ \frac{\sqrt{\alpha^2-\sigma^2}}{\sqrt{\eta_j^2-\sigma^2}}\sin t_j\sqrt{\eta_j^2-\sigma^2} & \cos t_j\sqrt{\eta_j^2-\sigma^2} \end{pmatrix},$$

при $1 < \sigma < \eta_j$, и

$$\begin{pmatrix} 1 & 0 \\ t_j\sqrt{\alpha^2-\eta_j^2} & 1 \end{pmatrix},$$

при $\sigma = \eta_j$.

Вектор $\vec{A}_j^o(\sigma)$ поворачивается при убывании σ от α до 1 по часовой стрелке начиная от положительного направления оси ординат на угол

$$P_A = \lim_{\sigma\to 1+0} \operatorname{arctg}\sqrt{\frac{\alpha^2-\sigma^2}{\sigma^2-\eta_{m+1}^2}}.$$

Годограф вектор-функции $\vec{a}_2(\sigma)$ есть четверть окружности радиуса α, проходимой против часовой стрелки при убывании σ от α до 1, начиная от положительного направления на оси абсцисс. Поскольку линейные преобразования $V_j(\sigma)$, унимодулярны, то вектор $\vec{a}_{j+1}(\sigma)$ ненулевой при любом $1 < \sigma < \alpha$. Пользуясь индукцией можно доказать следующую теорему.

Теорема. *Любой из векторов $\vec{a}_j(\sigma)$, $2 < j < m+1$ поворачивается монотонно против часовой стрелки, начиная от положительного направления на оси абсцисс, при убывании σ от α до 1.*

Поворот p_{m+1} вектора $\vec{a}_{m+1}(\sigma)$ при убывании σ от α до 1 можно подсчитать индуктивно. (Отметим, что здесь возникают определённые сложности из-за разрывности семейств преобразований $V_j(\sigma)$ при $\sigma \to \alpha$.) Тогда поворот вектора $\vec{a}_{m+1}(\sigma)$ относительно вектора $\vec{A}_m^o$ равен $p_{m+1} + P_A$. При этом векторы $\vec{a}_{m+1}(\sigma)$ и $\vec{A}_m^o$ образуют прямой угол, если не учитывать прямой угол, получающийся при $\sigma = \alpha$, число раз равное

$$K = \left[\frac{p_{m+1} + P_A}{\pi} \right]_- ,$$

где $[x]_-$ — наибольшее целое число строго меньшее x. Это и есть число собственных TE-волн, возможных в данном волноводе.

Работа выполнена при поддержке РФФИ грант 08-01-90102-Мол.

Список литературы

1. Борн М., Вольф Э. Основы оптики. — М.: Наука, 1970.

2. Ковалев М. Д. Многослойная модель в оптике и квантовой механике // ЖВМ и МФ. — 2009. — Т. 49, № 8. — С. 1–14.

3. Ковалев М. Д. Число TE- и TM-мод в многослойном планарном волноводе со слоями двух типов // Электромагнитные волны и электронные системы. — 2009. — Т. 14, № 2. — С. 4–17.

ПРАВИЛЬНЫЕ И БИПРАВИЛЬНЫЕ РАЗБИЕНИЯ

Е. В. Коломейкина (Москва)

Одним из основных объектов геометрии чисел являются целочисленные решетки. Обобщением решеток являются правильные системы точек, которые теснейшим образом связаны с правильными разбиениями пространства (разбиениями, обладающими транзитивной группой симметрий). Транзитивность действия группы симметрий на множестве ячеек разбиения означает, что для любых двух ячеек разбиения найдется движение, переводящее одну ячейку в другую и при этом все разбиение в себя.

Если группа симметрий разбиения представляет собой только группу трансляций, то мы имеем дело с разбиением пространства на параллелоэдры. Мы рассматриваем только нормальные разбиения пространства, т. е. такие разбиения, ячейки которых либо не пересекаются вовсе, либо пересекаются по целым общим граням.

Из определения правильности разбиения следует, что окрестности любого определенного радиуса в правильном разбиении попарно идентичны.

Главной задачей локальной теории является задача: конгруэнтность корон какого радиуса влечет правильность всего разбиения? Первый такой локальный критерий был доказан в 1976 году для точечных систем и для разбиений пространств постоянной кривизны и назван локальной теоремой:

Теорема [1] (локальная теорема). *Разбиение T пространства X^d постоянной кривизны правильно тогда и только тогда, когда найдется натуральное число k такое, что:*

1) *все короны радиуса k попарно конгруэнтны;*

2) *для любой ячейки $P \in T$ выполняется $S_{k-1}(P) = S_k(P)$, где $S_k(P)$ означает группу симметрий короны радиуса k ячейки P.*

Возникает вопрос поиска наименьшего радиуса конгруэнтности корон, обеспечивающего правильность разбиений.

Для разбиений евклидовой плоскости наименьший радиус конгруэнтности равен единице, что следует из теоремы [2] Н. П. Долбилина и Д. Шаттшнайдер, которая утверждает, что для правильности разбиения евклидовой плоскости необходимо и достаточно попарной конгруэнтности всех полных корон радиуса 1.

Определение. *Полной короной радиуса* 1 некоторой ячейки разбиения будем называть совокупность ячеек разбиения, смежных с данной ячейкой как по сторонам, так и по вершинам.

Определение. *Неполной короной радиуса* 1 некоторой ячейки разбиения будем называть совокупность ячеек разбиения, смежных с данной ячейкой (*центром* короны) только по сторонам.

Определение. Две короны *конгруэнтны*, если существует движение, которое переводит одну корону в другую и центр первой короны в центр второй короны.

Для случая евклидовой плоскости мы ослабляем условие попарной конгруэнтности полных корон радиуса 1 и заменяем его условием попарной конгруэнтности неполных корон. Таким образом, верна следующая

Теорема 1. *Разбиение евклидовой плоскости является правильным тогда и только тогда, когда все неполные короны радиуса* 1 *попарно конгруэнтны.*

Этот же факт оказывается верен и для двумерной сферы.

Теорема 2. *Разбиение двумерной сферы является правильным тогда и только тогда, когда все неполные короны радиуса* 1 *попарно конгруэнтны.*

Интересно, что аналогичный факт для плоскости Лобачевского уже не верен. Существует разбиение К. Берецки плоскости Лобачевского, в котором как все полные, так и неполные короны радиуса 1 попарно конгруэнтны, однако, разбиение правильным не является. Также не хватает условия конгруэнтности полных корон радиуса 1 и для обеспечения правильности разбиения евклидова пространства размерности 3 (разбиение П. Энгела).

Позднее результат локальной теоремы был обобщен Н. П. Долбилиным и М. И. Штогриным [3] на случай *мультиправильных* или

m–эдральных разбиений (разбиений, множество ячеек которых распадается в m орбит относительно группы симметрий разбиения). Обозначим через N_i — число классов неполных корон радиуса i.

Теорема (обобщенная локальная теорема). *Для $m \in N$ разбиение T является m-эдральным тогда и только тогда, когда найдется такое $k \in N$, что выполняется:*

1) $N_{k-1} = N_k = m$;

2) *для любого $P \in T$ выполняется $S_{k-1}(P) = S_k(P)$.*

Локальная теорема для правильных разбиений является частным случаем обобщенной локальной теоремы при $m = 1$.

Определение. Разбиение называется *биправильным*, если ячейки разбиения распадаются в 2 орбиты относительно группы симметрий разбиения.

Теорема 3. *Триангуляция евклидовой плоскости является биправильной тогда и только тогда, когда число N_1^* классов полных корон радиуса* 1 *в триангуляции равно* 2.

Эта теорема неулучшаема в том смысле, что 2 класса неполных корон радиуса 1 не гарантируют биправильность разбиения. Доказательство теоремы 3 переносится и на случай триангуляций двумерной сферы.

Теорема 4. *Триангуляция двумерной сферы является биправильной тогда и только тогда, когда число N_1^* классов полных корон радиуса* 1 *в триангуляции равно* 2.

Список литературы

1. Делоне Б. Н., Долбилин Н. П., Штогрин М. И., Галлиулин Р. В. Локальный критерий правильности системы точек // ДАН СССР. — 1976. — Т. 227, № 1. — С. 319–322.

2. Dolbilin N. P., Schattschneider D. One corona is enough for the Euclidean plane // Fields institute monographs quasi crystals and discrete geometry. — A.M.S., Rod Island, 1998. — P. 207–246.

3. Долбилин Н. П., Штогрин М. И. Локальный критерий для кристаллической структуры // IX Всесоюзная геометрическая конференция. — Кишинев, 1987. — Т. 64. — С. 99.

4. Коломейкина Е. В. О локальных условиях биправильных триангуляций евклидовой плоскости // Материалы IX Международного семинара "Дискретная математика и ее приложения", посвященного 75-летию со дня рождения академика О. Б. Лупанова (18–23 июня 2007 г.). — М.: Изд-во механико-математического факультета МГУ, 2007. — С. 384–386.

О ЧИСЛЕ ВНУТРЕННИХ ТОЧЕК В ТЕОРЕМАХ ЭРДЕША—СЕКЕРЕША

В. А. Кошелев (Москва)

В 1935 году П. Эрдеш и Д. Секереш сформулировали следующую проблему [1].

Первая проблема Эрдеша—Секереша. Для любого целого $n \geq 3$ найти минимальное положительное число $g(n)$, такое, что из любого множества точек на плоскости, находящегося в общем положении и содержащего по крайней мере $g(n)$ точек, можно выбрать подмножество мощности n, элементы которого являются вершинами выпуклого n-угольника.

В 1978 году Эрдеш предложил следующую модификацию первой проблемы.

Вторая проблема Эрдеша—Секереша. Для любого целого $n \geq 3$ найти минимальное положительное число $h(n)$, такое, что из любого множества точек $\mathcal{X}$ на плоскости, находящегося в общем положении и содержащего по крайней мере $h(n)$ точек, можно выбрать подмножество мощности n, элементы которого являются вершинами выпуклого и пустого n-угольника, т. е. этот n-угольник не содержит внутри себя других точек из $\mathcal{X}$.

Перечисленные проблемы являются классическими в комбинаторной геометрии и теории Рамсея. Обе они обобщаются следующим образом.

Третья проблема типа Эрдеша—Секереша. Для любых целых $n \geq 3$ и $k \geq 0$ найти минимальное положительное число $h(n,k)$, такое, что из любого множества точек $\mathcal{X}$ на плоскости, находящегося в общем положении и содержащего по крайней мере $h(n,k)$ точек, можно выбрать подмножество мощности n, элементы которого являются вершинами выпуклого n-угольника C с условием $|(C \setminus \partial C) \cap \mathcal{X}| \leq k$, т. е. этот n-угольник содержит внутри себя не более k других точек из $\mathcal{X}$.

Для первой проблемы Эрдеша—Секереша известно, что

$$g(3) = 3, \quad g(4) = 5, \quad g(5) = 9 \text{ [1]}, \quad g(6) = 17 \text{ [2]}$$

(последний результат был доказан совсем недавно и значительно позже предыдущих, с применением компьютерного перебора). В общем случае известно, что

$$2^{n-2} + 1 \leq g(n) \leq \binom{2n-5}{n-3} + 1.$$

Вторая проблема изучена более глубоко. Для нее доказаны следующие результаты:

$$h(3) = 3, \quad h(4) = 5, \quad h(5) = 10, \quad 30 \le h(6) \le 463,$$

и, наконец, при $n \ge 7$ величина $h(n)$ не существует [3]. Именно в связи с этим возникает третья проблема и, в частности, вопрос о существовании величины $h(n,k)$ при $n > 7$.

Для третьей проблемы, как нетрудно видеть, всегда выполнены неравенства

$$g(n) = h(n, g(n) - n) \le \ldots \le h(n,k) \le \ldots \le h(n,1) \le h(n,0) = h(n),$$

если соответствующие выражения существуют. Для малых значений n очевидны следующие результаты:

$$h(3,k) = 3, \quad h(4,k) = 5, \quad h(5,0) = 10, \quad h(5, \ge 1) = 9.$$

Последний результат обусловлен тем, что выпуклый пятиугольник с двумя или более точками внутри всегда содержит меньший выпуклый пятиугольник. Специальный алгоритм перебора, схожий с алгоритмом Секереша, Б. МакКея и Л. Питерса [2] может быть применен для компьютерного доказательства того, что $h(6, \ge 2) = 17$ и $h(6,1) = 18$.

Для произвольного n интересны ответы на вопросы о значениях $k = k(n)$ при которых $h(n,k)$ существует или не существует, а также $h(n,k) = g(n)$ или $h(n,k) > g(n)$ (поскольку точные значения $g(n)$ неизвестны, то аналогичные вопросы можно поставить заменив $g(n)$ на $2^{n-2} + 1$). Как было впервые установлено автором [4], последнее неравенство всегда выполнено при $k \le \binom{(n-3)}{\lceil (n-3)/2 \rceil} - \lceil \frac{n}{2} \rceil$.

Значения k при которых $h(n,k)$ не существует впервые изучались в статье Бл. Сендова. Сендов, используя множество Хортона [3], с помощью которого было доказано несуществование $h(7)$, доказал некоторую оценку для k следующего вида $k \le (\sqrt[4]{2} + o(1))^n$. Немного лучшие результаты были получены позже Е. Ныкловой, но асимптотика осталась без изменения. Недавно автором было доказано, что на самом деле, для несуществования $h(n,k)$ заведомо можно взять $k \le (2 + o(1))^n$, а именно $\binom{(n-7)}{(n-7)/2} - 1$ для нечетных n и $2\binom{(n-8)}{(n-8)/2} - 1$ для четных [4].

В связи с проблемами Эрдеша—Секереша очень часто рассматривают выпуклые ломаные, которые были предложены самими

авторами задач в [1] и которые принято называть "чашками" и "крышками". Напомним их определение. Пусть на плоскости дана система координат. Множество точек $(x_1, y_1), \ldots, (x_n, y_n)$ называется *n-чашкой*, если $x_1 < \ldots < x_n$ и $\frac{y_1-y_2}{x_1-x_2} < \frac{y_2-y_3}{x_2-x_3} < \ldots < \frac{y_{n-1}-y_n}{x_{n-1}-x_n}$. Если в последнем неравенстве заменить все знаки на больше, то это множество будет *n-крышкой*.

Следуя Эрдешу и Секерешу, обозначим через $f(l, m)$ минимальное положительное число, такое, что из любого множества точек на плоскости, находящегося в общем положении, не содержащего пары точек с одинаковыми абсциссами, и имеющего мощность $f(l, m)$ или более, всегда можно выбрать подмножество, образующее либо l-чашку, либо m-крышку. Задача отыскания величины $f(l, m)$ была полностью решена Эрдешем и Секерешем в 1961 году. Они показали, что $f(l, m) = \binom{l+m-4}{l-2} + 1$.

Для чашек и крышек можно сформулировать задачи, аналогичные тем, которые мы обсуждали для $h(n, k)$, и определить соответствующую величину $f(l, m, l', m')$. Для этих задач автором тоже были получены сильные оценки [4].

Работа выполнена при финансовой поддержке гранта РФФИ 09-01-00294.

Список литературы

1. Erdős P., Szekeres G. A combinatorial problem in geometry // Compositio Math. — 1935. — V. 2. — P. 463–470.

2. Szekeres G., Peters L. Computer solution to the 17-point Erdős—Szekeres problem // ANZIAM J. — 2006. — V. 48. — 151–164.

3. Horton J. D. Sets with no empty 7-gons // Canad. Math. Bull. — 1983. — V. 26. — P. 482–484.

4. Koshelev V. A. On Erdős–Szekeres problem and related problems // http://arxiv.org/PS_cache/arxiv/pdf/0910/0910.2700v1.pdf

О ХРОМАТИЧЕСКИХ ЧИСЛАХ НЕКОТОРЫХ ГЕОМЕТРИЧЕСКИХ ФРАКТАЛОВ

О. В. Кузьмин, А. О. Малакичев (Иркутск)

Хроматическим числом пространства называется величина, равная минимальному количеству цветов, в которые можно раскрасить все точки пространства так, чтобы никакие две точки одного цвета

не находились на расстоянии, равном 1. В действительности хроматическое число пространства не изменится, если в качестве запрещенного расстояния выбрать любое другое фиксированное число. Нахождение хроматического числа пространства — одна из сложнейших и важнейших задач комбинаторной геометрии. Много различных результатов этой области математики приведено в работах А. М. Райгородского (см., напр., [1]).

Не менее интересной представляется задача нахождения хроматических чисел фрактальных множеств. В данной работе рассматривается задача нахождения хроматического числа геометрического фрактала, а также соответствующего ему фрактального графа на примере одного из „классических“ фрактальных множеств.

Рассмотрим „салфетку Серпинского“ — геометрический фрактал, обладающий свойством идеального самоподобия. Один из алгоритмов построения этого фрактала заключается в следующем. Пусть S_0 – правильный треугольник. Разделим его средними линиями на четыре равных треугольника. Удаляя внутренность центрального из треугольников, получим множество S_1, состоящее из трех правильных треугольников. Продолжив аналогичную операцию с оставшимися треугольниками, получим множество S_n, где $n \in N$ — количество итераций, являющееся предфракталом. Тогда „салфетка Серпинского“ есть множество $S = \bigcap\limits_{n=1}^{\infty} S_n$ [2].

Рассмотрим задачу о раскраске „салфетки Серпинского“. Будем считать, что множество S лежит на плоскости, с заданной на ней евклидовой метрикой. В силу самоподобия множества S, свойства предфрактала S_n будут распространяться и на „салфетку“. Таким образом, задача о нахождении хроматического числа множества S сводится к решению проблемы о раскраске множества S_n. Запрещенным расстоянием в данной задаче будем считать длину стороны треугольника, получающегося при каждой итерации.

Опишем процесс раскраски S_n. Раскраску начнем с треугольника S_0, вершины которого обозначим $A_1A_2A_3$. Всем точкам треугольника S_0, кроме A_2 и A_3, присвоим „первый“ цвет. Точке A_2 присвоим „второй“ цвет, а точке A_3 — „третий“. При такой раскраске никакие две точки треугольника, находящиеся на запрещенном расстоянии, не окрашены в один цвет. После первой итерации мы получим три треугольника $A_1A_2A_3$, $A_2A_4A_5$ и $A_3A_5A_6$. Каждую точку треугольников $A_2A_4A_5$ и $A_3A_5A_6$, кроме A_4, A_5 и A_6 раскрасим во „второй“ и „третий“ цвета соответственно. Точки A_4 и A_5 раскрасим в „первый“ цвет. При такой раскраске точка A_5 не может быть раскрашена в те же цвета, что и точки A_2, A_3, A_4 и A_6, так как расстояние между ними равно длине стороны треугольника первой итерации.

Кроме того, точке A_5 не может быть присвоен „первый“ цвет, так как в треугольнике $A_1A_2A_3$ найдутся точки, лежащие на запрещенном расстоянии от A_5 и имеющие „первый“ цвет. Значит, точка A_5 будет окрашена в „четвертый“ цвет. Таким образом, хроматическое число предфрактала S_1 равно 4. Искомая раскраска будет получена, если на последующих итерациях мы продолжим присваивать каждому новому треугольнику цвет по правилу, описанному выше. Тем самым доказана

Теорема 1. *Хроматическое число „салфетки Серпинского“ равно* 4.

„Салфетке Серпинского“ поставим в соответствие граф, который строится следующим образом. Каждый треугольник „салфетки“ заменяется на вершину графа; если у двух треугольников была общая точка, то соответствующие им вершины графа соединяем ребром. При таком построении множеству S_0 будет соответствовать граф G_0, состоящий из одной вершины; множеству S_1 — граф G_1, состоящий из трех вершин и трех ребер и т. д. Предфракталу S_n будет соответствовать циклический граф G_n, где $n \in N$, состоящий из 3^n вершин и $\frac{3}{2}(3^n - 1)$ ребер. Множеству S соответствует бесконечный граф G.

Граф G является фрактальным. Действительно, G можно построить из графа G_0, с помощью затравки $H = (W, Q)$, где $W = \{w_1, w_2, w_3\}$, $Q = \{(w_1, w_2); (w_1, w_3); (w_2, w_3)\}$ (см. [3]). Процедура замены вершины затравкой будет производится следующим образом. В графе G_0 вершина заменяется на затравку H. Далее совершаем циклический обход графа G_1, заменяя каждую его вершину на затравку H, получим граф, соответствующий второй итерации „салфетки“. Продолжая данную операцию, мы построим фрактальный граф, соответствующий „салфетке Серпинского“.

Для нахождения хроматического числа графа G достаточно найти хроматическое число графа G_n. Вершине w_1 затравки H присвоим „первый“ цвет, вершине w_2 — „второй“, w_3 — „третий“. При построении G_n будем использовать затравку с „раскрашеными“ вершинами, тогда после каждой итерации хроматическое число графа G_n остается равным 3, следовательно, хроматическое число G равно 3. Тем самым доказана

Теорема 2. *Хроматическое число графа, соответствующего „салфетке Серпинского“, равно* 3.

Список литературы

1. Райгородский А. М. Хроматические числа. — М.: МЦНМО, 2003.

2. Кроновер Р. М. Фракталы и хаос в динамических системах. Основы теории. — М.: Постмаркет, 2000.

3. Кочкаров А. А., Кочкаров Р. А. О планарности и других топологических свойствах фрактальных графов // Препринт ИПМ им. М. В. Келдыша РАН № 83. — М., 2003.

ИЗОЭДРАЛЬНЫЕ РАЗБИЕНИЯ ТРЁХМЕРНОЙ СФЕРЫ И ЗАКОНОМЕРНОСТИ ВЗАИМНЫХ ОРИЕНТАЦИЙ КРИСТАЛЛОВ

Я. В. Кучериненко (Москва)

Работа посвящена описанию некоторых особенностей изоэдральных разбиений Дирихле—Вороного трёхмерной сферы, которые соответствуют выбору особо симметричных точек этой сферы, повторяемых теми специальными точечными группами этой сферы, которые соответствуют описаниям взаимных ориентаций кристаллов.

Пусть имеется пара кристаллов A и B с группами симметрии $\{a_i\}$ и $\{b_i\}$. В работе [1] показано, что описание их взаимных ориентаций сводится к описанию области Дирихле—Вороного (на трёхмерной сфере) относительно орбиты некоторой дискретной группы, порождённой некоторым специальным образом при помощи групп $\{a_i\}$ и $\{b_i\}$. Описание этой группы получается достаточно просто, если использовать алгебру кватернионов и представлений с их помощью трёхмерных точечных групп $\{a_i\}$ и $\{b_i\}$ — эта алгебра широко известна из работ Гамильтона, Кейли и Клейна (например, см. [2–7]), а применительно к нашим проблемам рассмотрена в [8–9]. В настоящей работе показаны следующие утверждения:

Область Дирихле—Вороного для точки, соответствующей тождественному движению, обладает центром симметрии. Совокупность этих областей образует разбиение Дирихле—Вороного, которое легко воссоздать при помощи геометрических операций группы симметрии в S^3. В свою очередь, с помощью построенного разбиения можно наглядно показать геометрическое действие групповых операций.

Стабилизатор орбиты изоморфен группе симметрии кристаллического двойника. С помощью разбиения Дирихле—Вороного в S^3 это можно довольно наглядно продемонстрировать.

Пусть для данных кристаллов (фигур) A и B известна их взаимная ориентация. Если кристаллы одинаковы, то смена порядка фигур в паре (A, B) никак не влияет на группу, действующую на сфере

S^3 ни на её орбиту. Если же кристаллы разные, то смена порядка фигур в паре (A, B) меняет все движения, описывающие взаимные ориентации кристаллов, на обратные им. При этом на сфере S^3 на орбиту соответствующих точек действует симметрия в точке. Таким образом смена порядка фигур не меняет структуру группы на S^3, а приводит к движению всей орбиты. Аналогично, смена начальных положений фигур приводит к повороту орбиты как целого, не меняя структуру группы. Обнаруженные факты позволяют описать взаимные ориентации не только одинаковых, но и разных кристаллов.

Если в паре (A, B) кристаллы одинаковы, то можно говорить о величине их разориентировки (например, разориентировку можно понимать как величину угла поворота, совмещающего один кристалл с другим), в том числе о максимально возможной разориентировке для заданной точечной группы симметрии. Если же в паре (A, B) кристаллы разные, то понятие "величина разориентировки" теряет смысл, поскольку нет однозначности в выборе начального взаимного расположения кристаллов. Однако есть возможность сравнивать степень различия взаимных ориентаций кристаллов в двух разных парах (A_1, B_1) и (A_2, B_2) (при условии что фигура A_1 конгруэнтна с A_2, а B_1 — с B_2). В обоих случаях максимальная разница ориентаций является диаметром орбифолда.

Переходя от описания взаимной ориентации пары сросшихся кристаллов к описаниям взаимных ориентаций кристаллических зёрен в материалах и горных породах, приходим к распределениям точек на S^3 (или, точнее, на орбифолде). Эти распределения, очевидно, обладают той же симметрией, что и рассмотренные выше орбиты. Области сгущения соответствуют наиболее часто встречающимся разориентировкам. Такой подход может предоставить дополнительные возможности в описании (и определении) свойств поликристаллических материалов и горных пород.

Изложенные результаты позволяют утверждать, что теория взаимных ориентаций кристаллов (в том числе в кристаллических двойниках) фактически является частью раздела классической геометрической кристаллографии посвященного четырёхмерным точечным группам симметрии (дискретным группам трёхмерной сферы).

Автор благодарит Виталия Сергеевича Макарова за помощь и обсуждение результатов.

Список литературы

1. Кучериненко Я. В. О взаимной ориентации двух фигур в R^3 // Материалы VII Международного семинара "Дискретная математика и ее приложения". Т. 2. — М., 2001. — С. 268–270.

2. Hamilton W. R. Letter to graves on quaternions; or on a new system of imaginaries in algebra // Phil. Mag. — 1844. — V. XXV. — P. 489–495.

3. Cayley A. On certain results relating to quaternions // Philosophical Magazine. — 1845. — V. XXVI. — P. 141–145.

4. Cayley A. On the homographic transformation of a surface of the second order into itself // Philosophical Magazine. — 1854. — V. VII. — P. 208–212.

5. Клейн Ф. Лекции об икосаэдре и решении уравнений пятой степени. — М.: Наука, 1989.

6. Goursat E. Sur les substitutions orthogonales et les divisions regulieres de l'espace // Annales scientifiques de l'ecole Normale Superieure. Ser. 3. — 1889. — V. 6. — P. 9–102.

7. Долбилин Н. П. О правильных разбиениях Дирихле сферы. — М., 1972.

8. Кучериненко Я. В. О взаимном расположении двух фигур в пространствах постоянной кривизны // Материалы VIII Международного семинара "Дискретная математика и ее приложения". — М., 2004. — С. 398–400.

9. Кучериненко Я. В. Повороты симметрии в трехмерном и четырехмерном пространствах // Труды IV Всероссийской научной школы "Математические исследования в кристаллографии, минералогии и петрографии" (27–28 октября 2008 г., Апатиты). — С. 25–32.

НОВЫЙ ПРАВИЛЬНЫЙ МНОГОГРАННИК

С. А. Лавренченко (Москва)

Понятие правильности зависит от того, насколько широк класс допускаемых к рассмотрению многогранников. Так, если мы ограничимся выпуклыми многогранниками в 3-мерном пространстве, существуют пять хорошо известных Платоновых многогранников. Если мы допустим многогранники с самопересечениями, то найдутся еще четыре правильных многогранника Кеплера-Пуансо. Мы же будем обобщать по другому направлению — не будем допускать самопересечений, но разрешим размерности объемлющего евклидового пространства увеличиваться. Мы будем рассматривать 2-мерные многогранники в 4-мерном пространстве. Тогда обнаруживается еще один правильный многогранник.

Триангуляция 2-мерной компактной поверхности — это симплициальный 2-комплекс, гомеоморфный (в качестве его носителя)

этой поверхности. *Автоморфизмом* триангуляции называется любая сохраняющая грани (т. е. 2-симплексы) перестановка множества ее вершин. Группа автоморфизмов триангуляции T обозначается $\mathrm{Aut}(T)$. *Полная группа симметрий* $\mathrm{Sym}(P)$ многогранника P в евклидовом n-мерном пространстве E^n определяется как множество всех евклидовых изометрий этого пространства, которые оставляют P инвариантным.

Говорят, что многогранник P *геометрически реализует* триангуляцию T в E^n, если P является образом вложения T в E^n, линейным на симплексах T. Автоморфизмы T, представленные симметриями многогранника P, называются *геометрически реализованными*.

Что же такое правильный многогранник? Что касается 2-мерных многогранников в E^n, давайте примем такое определение.

Правильным многогранником будем называть многогранник, полная группа симметрий которого вершинно-, реберно-, гранево- или флагово-транзитивна. В зависимости от степени транзитивности, многогранник будет называться вершинно-правильным, реберно-правильным, гранево-правильным или флагово-правильным.

У вершинно-правильного многогранника многогранные углы при всех вершинах конгруэнтны, у реберно-правильного двугранные углы при всех ребрах конгруэнтны, у гранево-правильного все грани конгруэнтны. Флагово-правильные многогранники обладают всеми перечисленными свойствами конгруэнтности.

Будем называть *абстрактным тороидальным гексадекаэдром* и обозначать ATH (abstract toroidal hexadecahedron) абстрактный симплициальный 2-комплекс с 8 вершинами и 16 гранями, который строится следующим образом. Обозначим его восемь вершин через a, b, c, d, e, f, g и h. Его 1-мерный скелет — полный четырехдольный граф $K_{2,2,2,2}$, в котором все пары вершин соединены ребрами (т. е. 1-симплексами), кроме следующих четырех противолежащих пар: $\{a,f\}$, $\{b,h\}$, $\{c,e\}$ и $\{d,g\}$. В этом графе $|E| = \binom{8}{2} - 4 = 24$ ребра. Список шестнадцати граней (2-симплексов) следующий:

abd, dbe, bef, bcf, cfd, cda, efg, ghf,
hfd, hde, ega, abg, bcg, ghc, cah, hea.

Можно проверить, что к каждому ребру примыкают ровно две грани и что в линке каждой вершины получается простой цикл длины 6. Эти линки просматриваются в схеме вращений графа:

$a : bgehcd$, $b : adefcg$, $c : bfdahg$, $d : acfheb$,
$e : agfbdh$, $f : beghdc$, $g : abchfe$, $h : aedfgc$.

Из сказаного следует, что симплициальный 2-комплекс ATH соответствует триангуляции замкнутой поверхности, в которой степень каждой вершины равна 6. Далее, поскольку число вершин $|V| = 8$, число ребер $|E| = 24$ и число граней $|F| = 16$, и поскольку $|V| - |E| + |F| = 8 - 24 + 16 = 0$, это триангуляция тора или бутылки Клейна, по формуле Эйлера. Однако, граф $K_{2,2,2,2}$ не укладывается на бутылке Клейна, потому что в [1] доказано, что никакой граф, в котором степень каждой вершины равна 6, не может быть одновременно и тороидальным и клейново-бутылочным. С другой стороны, $K_{2,2,2,2}$ укладывается на торе; см. [2]. Таким образом, ATH — действительно триангуляция тора.

Все автоморфизмы группы Aut(ATH) определены в [3]. Эта группа порождается инволюциями $\theta_1 = (ce)(dg)$ и $\theta_2 = (af)(cg)(de)$ в комбинации с единым циклическим сдвигом всех вершин $\sigma = (aebgfchd)$. Инволюции θ_1 и θ_2 порождают стабилизатор вершины h. С другой стороны, наличие сдвига σ обеспечивает вершинную транзитивность группы. Поэтому $|\mathrm{Aut}(\mathrm{ATH})| = 2 \cdot 2 \cdot 8 = 32$.

Теорема. *В евклидовом 4-мерном пространстве существует 2-мерный многогранник с 8 вершинами и 16 треугольными гранями без самопересечений, который одновременно вершинно-правильный и гранево-правильный.*

(Этот многогранник будет называться правильным тороидальным гексадекаэдром и обозначаться RTH (regular toroidal hexadecahedron).)

Доказательство. Вершинная транзитивность группы Aut(ATH) была показана выше. Транзитивность на гранях проверяется непосредственно.

Чтобы реализовать триангуляцию ATH в E^4 геометрически (без самопересечений!), мы вложим ее в 2-мерный скелет 4-мерного гипероктаэдра так, что каждая грань реализуется геометрическим 2-симплексом последнего. Для этого поместим восемь вершин ATH в восемь вершин гипероктаэдра следующим образом:

$A\,(0,\,0,\,0,\,1)$, $B\,(1,\,0,\,0,\,0)$, $C\,(0,\,0,\,-1,\,0)$, $D\,(0,\,-1,\,0,\,0)$,
$E\,(0,\,0,\,1,\,0)$, $F\,(0,\,0,\,0,\,-1)$, $G\,(0,\,1,\,0,\,0)$, $H\,(-1,\,0,\,0,\,0)$,

где каждая точка изображает вершину триангуляции, обозначенную той же буквой алфавита (но строчной). Таким образом все грани ATH реализуются конгруэнтными правильными треугольниками со стороной $\sqrt{2}$.

Образующие перестановки θ_1, θ_2 и σ группы Aut(ATH) нетрудно реализовать геометрически матрицами 4×4 и убедиться, что получаются ортогональные матрицы. Таким образом, группа Aut(ATH)

точно представима в 4-мерном пространстве дискретной группой движений, порожденной этими тремя ортогональными матрицами, т. е. группой Sym(RTH). Таким образом, группа Sym(RTH) вершинно- и гранево-транзитивна, как и группа Aut(ATH). Теорема доказана.

Список литературы

1. Lawrencenko S., Negami S. Constructing the graphs that triangulate both the torus and the Klein bottle // J. combinatorial theory, series B. — 1999. — V. 77, I. 1. — P. 211–218.

2. Лавренченко С. А. Неприводимые триангуляции тора // Укр. геометр. сборник. — 1987. — Вып. 30. — С. 52–62.

3. Лавренченко С. А. Перечисление в явном виде всех автоморфизмов неприводимых триангуляций тора и всех укладок на тор помеченных графов этих триангуляций // Деп. в УкрНИИНТИ 01.10.87, № 2779–Ук87. — Харьков, 1987.

О ЧИСЛЕ КЛАССОВ БИЛИПШИЦЕВОЙ ЭКВИВАЛЕНТНОСТИ МНОЖЕСТВ ДЕЛОНЕ

А. Н. Магазинов (Москва)

Настоящая работа посвящена устройству дискретных множеств с точки зрения их билипшицевой эквивалентности. Вопрос о билипшицевой эквивалентности двух множеств Делоне был поставлен М. Громовым в работе [1].

Пусть M — метрическое пространство. Множество $\mathcal{A} \subset M$ является (r, R)-*множеством Делоне* для некоторых $0 < r < R$, если выполняются следующие 2 условия:

1) Для любых x, y, принадлежащих $\mathcal{A}$, выполнено
$$B_r^\circ(x) \bigcap B_r^\circ(y) = \varnothing;$$
2) $\bigcup\limits_{x \in \mathcal{A}} B_R(x) = M$.

Здесь $B_\rho(x)$ и $B_\rho^\circ(x)$ означают соответственно замкнутый и открытый шары радиуса ρ с центром в точке x. Множество $\mathcal{A}$ будем называть просто множеством Делоне, если для некоторых $0 < r < R$ оно является (r, R)-множеством Делоне.

Пусть имеется пара точек $x, y \in M$. Будем обозначать через $|x - y|$ расстояние между точками x и y. Если же M нормировано над $\mathbb{R}$, то через $(x - y)$ будем обозначать вектор с началом в y и концом в x.

Два множества Делоне $\mathcal{A}$ и $\mathcal{B}$ называются *билипшицево эквивалентными*, если существует константа $\lambda \geqslant 1$ и биекция $F : \mathcal{A} \to \mathcal{B}$ такая, что для любых $x, y \in \mathcal{A}$ выполнено неравенство

$$\frac{1}{\lambda}|x - y| \leqslant |F(x) - F(y)| \leqslant \lambda|x - y|.$$

Отображение F, для которого выполнено такое неравенство, называется λ-*билипшицевым*.

В случае евклидова пространства $\mathbb{E}^d$ Д. Бураго и Б. Кляйнером был получен [2] следующий результат:

Теорема 1. *В евклидовой плоскости $\mathbb{E}^2$ существует множество Делоне $\mathcal{A}$, не являющееся билипшицево эквивалентным решетке $\mathbb{Z}^2$.*

Как указывают авторы, аналогичная теорема может быть доказана для любой размерности $d \geqslant 2$. Таким образом установлено, что в евклидовом пространстве размерности $d \geqslant 2$ существуют как минимум 2 класса билипшицевой эквивалентности.

В доказательстве использована вспомогательная теорема:

Теорема 2. *Пусть $I = [0, 1]$. Для любого $c > 1$ найдется непрерывная функция $\rho : I^2 \to [1, c]$ такая, что не существует отображения $f : I^2 \to \mathbb{E}^2$, для которого $\det Df = \rho$ почти всюду на I^2.*

Основной результат, формулируемый в настоящем докладе, следующий:

Теорема 3. *Множество классов билипшицевой эквивалентности множеств Делоне в $\mathbb{E}^d$ имеет мощность континуум.*

Верхняя оценка мощности следует из результата А. Гарбера [3] об универсальности $\mathbb{Z}^d$.

Для получения нижней оценки достаточно рассмотреть некоторый специальный класс множеств Делоне.

Множество Делоне $\mathcal{A}$ называется L-*специальным*, если существует разбиение $\mathbb{E}^d$ на кубы с ребрами длины не меньшей 1 и не большей L и параллельными осям координат такое, что $\mathcal{A}$ — в точности множество вершин кубов разбиения с наименьшей для своего куба суммой координат.

Точка специального множества Делоне называется *стандартной*, если она соответствует кубу с ребром, равным 1, и *исключительной* в противном случае.

При построении континуального семейства неэквивалентных множеств используется дискретный аналог теоремы 2.

Теорема 2'. *Пусть даны $\lambda \geqslant 1$, $L \geqslant 1$ и рациональное $c > 1$. Тогда найдется дискретное множество $\mathcal{B}_0 = \mathcal{B}_0(\lambda, L, c)$ такое, что:*

1) *найдется полуоткрытый параллелепипед* Π *с целыми ребрами, параллельными координатным осям, и отмеченной вершиной и с наименьшей суммой координат такой, что* $\mathcal{B}_0 \subset \Pi$*;*

2) *существует разбиение* Π *на кубы с ребрами 1 и с. Множество ближайших к и вершин кубов равно* $\mathcal{B}_0$*;*

3) *для каждого множества Делоне* $\mathcal{B}$ *такого, что* $\mathcal{B} \cap \Pi = \mathcal{B}_0$ *и для любой* λ*-билипшицевой биекции* $F : \mathcal{B} \to \mathcal{A}$ *с* L*-специальным множеством* $\mathcal{A}$ *множество* $F(\mathcal{B}_0)$ *содержит хотя бы одну исключительную точку.*

Список литературы

1. Gromov M. Asymptotic invariants for infinite groups // London Mathematical Society Lecture Notes. — 1993. — V. 182. Geometric group theory.

2. Burago D., KleinerB. Separated nets in Euclidean space and Jacobians of bi-Lipschitz maps // Geom. Funct. Anal. — 1998. — V. 8. — P. 273–282.

3. Гарбер А. И. О классах эквивалентности множеств Делоне // Моделирование и анализ информационных систем. — 2009. — Т. 16, вып. 2. — С. 109–118.

ОБ A-РАЗБИЕНИЯХ ПЛОСКОСТИ ЛОБАЧЕВСКОГО

П. В. Макаров (Москва)

Условимся архимедовым разбиениям (коротко — A-разбиением) пространства постоянной кривизны называть (нормальное) разбиение пространства на неравные правильные многогранники, группа симметрии которого действует транзитивно на множестве вершин разбиения. Нормальное разбиение пространства на равные правильные многогранники условимся называть платоновым разбиением. Их перечень содержится в [1].

Для вывода архимедовых многогранников из правильных обычно применяются некоторые стандартные методы. Простейший из них — метод усечения вершин. Из каждого платонова многогранника $\{p, q\}$ этим методом образуется архимедов многогранник $(2p, 2p, q)$, (например из симплекса $\{3, 3\}$ — усеченный симплекс $(6, 6, 3)$, и т. п.). Аналогичная операция, проделанная над правильным многогранником $\{p, q\}$, вписанным в эквидистантную поверхность, приводит к архимедову многограннику $(2p, 2p, q)$ также вписанному в эквидистантную поверхность. Его проекция на базовую

плоскость дает A-разбиение $(2p, 2p, q)$ этой плоскости (условимся говорить, что оно получено из платонова разбиения $\{p, q\}$ путем усечения вершин). Если усечение вершин проводить так, чтобы усекающие плоскости проходили через центры ребер (центрореберное усечение), то мы из платонова разбиения $\{p, q\}$ получим почти правильное разбиение $\{p, q, p, q\}$, т. е. из правильного многогранника — почти правильный. Легко проверяется, что и все остальные методы получения архимедовых многогранников (разбиений) из платоновых также переносятся и на рассматриваемый класс бесконечных правильных многогранников пространства Лобачевского. Из платонова многогранника $\{p, q\}$ получаются архимедовы многогранники $(4, 2p, q)$, $(p, 4, q, 4)$, $(p, 3, q, 3, 3)$. Аналогично применяются эти методы и к правильным многогранникам с бесконечными гранями. Некоторые из рассмотренных методов допускают естественные обобщения. Так появляются A-разбиения $(p, q, p, q, \ldots, p, q)$, $(q, 2p, k, 2p)$ и $(3, q, 3, p, 3, p)$. Естественно встает вопрос: нет ли еще каких-нибудь серий A-разбиений (многогранников)? Вспоминая одну из конструкций, использованную в [2], которую, исходя из наших задач, можно сформулировать так:

Теорема 1. *Пусть нам задано k четных натуральных чисел, $k > 3$, $2p_1$, $2p_2$,..., $2p_k$, $2p_i \geq 2$. Тогда существует A-разбиение плоскости Лобачевского Λ^2, в звезде узла которого сошлись $2p_i$-угольники, $i = 1,\ldots, p$, в указанной последовательности (такое разбиение единственное, если все числа набора — разные).*

Возникает вопрос: нельзя ли в набор четных чисел добавить хоть одно нечетное? И следующий вопрос — о числе нечетноугольников, которые могут встретиться в одной вершине. Но до этого полезно убедиться (тем же методом) в существовании произвольной звезды:

Теорема 2. *Если нам задан набор натуральных чисел p_1, p_2, ..., p_k, где $k > 6$, то на Λ^2 существует звезда, состоящая из k правильных p_i-угольников, $i = 1,\ldots, k$, в которой p_i-угольники сходятся в заданной нам последовательности (число k может быть уменьшено, если p_i достаточно велики; например, если все $p_k \geq 7$, то в качестве k достаточно взять число 3).*

Идя тем же путем, не сложно доказать утверждение:

Теорема 3. *Каков бы ни был наперед заданный (конечный) набор из k правильных нечетноугольников, его всегда можно пополнить не более чем $3k$ четноугольниками так, что из полученного набора можно построить звезду A-разбиения и его самого.*

Дальнейшее продвижение в этом же направлении в определенной степени теряет смысл в связи со следующей теоремой:

Теорема 4. *Каков бы ни был заданный набор из k правильных многоугольников, он всегда может быть пополнен единственным правильным p-угольником, $p \leq 5$, так, что из пополненного набора можно построить звезду, являющуюся звездой A-разбиения плоскости Лобачевского.*

Доказательство. Склеим поочередно по стороне все заданные нам многоугольники, вытянув их, для простоты, в линейную цепочку. Рассмотрим объединение всех многоугольников полученного комплекса (считая, для простоты, $p_i \geq 4$). Отметим, что полученный многоугольник можно считать выпуклым. Пусть число α_1 сравнимо с числом q по модулю 4, $\alpha_1 = 4s+q \equiv (\mathrm{mod}\ 4)$. Если $q \neq 0$, то приклеив к полученному многоугольнику еще и правильный p_{k+1}-угольник, где $p_{k+1} = 6-q$, мы, после этой приклейки, получим многоугольник с числом сторон $4s + q(6-q) - 2 = 4(s+1)$. Таким образом, число сторон нового многоугольника будет кратно 4. Все его стороны равны по длине (а углы можно считать острыми). Как и в предыдущих примерах, сумму углов нового многоугольника можно сделать равной 2π. Но каноническое отождествление (как "ручечное", так и противоположных сторон) порождает единственный цикл вершин (в смысле А. Пуанкаре [3]) и при том неособенный. Иными словами, дискретная группа Г, порожденная движениями, канонически отождествляющими стороны построенного $4(p+1)$-угольника, действует однотранзитивно на множестве вершин этого многоугольника. Занумеровав вершины $4p$-угольника и выписав единственный (неособенный) цикл вершин, мы сможем выписать и последовательность схождения составляющих p_i-угольников, $i = 1, \ldots, k+1$, в вершине звезды. Замечание: если $q = 0$, то можно дополнительного многоугольника и не прикладывать.

Легко заметить, что многоугольники, из которых образован $4(p+1)$-угольник, можно переставлять в линейной последовательности, можно "проворачивать" их друг относительно друга, можно нарушать и линейность склейки (до определенных границ). Все это приводит, вообще говоря, к другим A-разбиениям плоскости Лобачевского (род p фуксовой группы и поверхности, соответствующих $4p$-угольнику, при этом сохраняется). Из приведенных примеров мы видим, что классификация A-разбиений более детальная, чем по родам соответствующих поверхностей (именно этой классификации придерживался А. Пуанкаре [3] в теории планигонов в Λ^2), видимо мало целесообразна, хотя для некоторых родов возможно имеет смысл перебрать все возможные отождествления, дающие A-разбиения с заданным набором p_i-угольников, и, возможно, пересмотреть все сорта Делоне таких A-разбиений.

Используя фактически теорему о продолжении [4] и предшествующие ей идеи А. Пуанкаре, изложенные в работе [3], можно в конкретной ситуации ответить на вопросы о существовании и о единственности A-разбиения с наперед заданной звездой.

Список литературы

1. Макаров В. С. О некоторых обобщенных правильных многогранниках пространства Лобачевского // Материалы IX Международного семинара "Дискретная математика и ее приложения", посвященного 75-летию со дня рождения акад. О. Б. Лупанова. — М.: Изд-во мех-мат ф-та МГУ, 2007. — С. 390–393.

2. Макаров В. С. Об одном классе двумерных федоровских групп // Изв. АН СССР. — 1967. — Т. 31, № 3. — С. 531–542.

3. Poincare H. Memoire sur les groupes fuchsciennes // Acta Math. — 1882. — V. 1. — P. 1–62.

4. Долбилин Н. П. О локальных свойствах дискретных правильных систем // Докл. АН СССР. — 1976. — Т. 230, № 3. — С. 516–519.

СИЛЬНАЯ ПРОБЛЕМА ТРИНАДЦАТИ ШАРОВ

О. Р. Мусин, А. С. Тарасов (Москва)

Рассмотри N точек на сфере $\mathbb{S}^2$. Обозначим через

$$d_N := \max_P \min_{i \neq j} \{angular\, dist(p_i, p_j)\},$$

где $P = \{p_1, \ldots, p_N\} \subset \mathbb{S}^2$. Другими словами, какое должно быть расположение N равных, не пересекающихся кругов, чтобы их общий радиус был максимальным? Этот вопрос, так же известный как проблема "враждующих диктаторов", был впервые поставлен голландским биологом Таммесом в 1930 году, который пришел к этой проблеме исследуя распределение пор на зернах пыльцы различных цветов.

К настоящему моменту проблема Таммеса была решена только для значений $N = 3, 4, 6, 12$ (Ласло Фейеш Тот, 1943), для $N = 5, 7, 8, 9$ (Шутте, ван дер Варден, 1951), $N = 10, 11$ (Данцер, 1963), $N = 24$ (Робинсон, 1961).

Первый нерешенный случай задачи Таммеса возникает при $N = 13$ и представляет особый интерес из-за со связи с контактным числом и гипотезой Кеплера о плотности упаковки шаров.

Знаменитая проблема 13 сфер заключается в том, могут ли 13 равных непересекающихся шаров в $\mathbb{R}^3$ касаться другого шара того же размера? Очевидно, этот вопрос эквивалентен неравенству $d_{13} < 60°$. Эта проблема была темой знаменитой дискуссии между Исааком Ньютоном и Дэвидом Грегори в 1694 году. Первое доказательство того, что $d_{13} < 60^0$ нашли Шутте и ван дер Варден только в 1953 году.

Это неравенство было усилено Бороцким и Сабо в 2003 году. Они доказали, что $d_{13} < 58,7°$. Недавно C. Bachoc и F. Valentin показали, что $d_{13} < 58,5°$.

Рассмотрим расположение 13 точек на единичной сфере. Проведем между двумя точками линию, если расстояние между ними равно минимальному расстоянию между точками. Мы получили граф G с 13 вершинами. Будем говорить, что граф G *неприводимый*, если смещение любой вершины графа G не увеличивает минимальное расстояние.

Хорошо известно расположение 13 точек на $\mathbb{S}^2$, для которого минимальное расстояние между точками этого расположения $\approx 57,1367°$.

Мы покажем, что это расположение является наилучшим.

Теорема. $d_{13} \approx 57,1367°$. *Расположение точек на сфере* $\mathbb{S}^2$ *с минимальным расстоянием между различными точками* d_{13} *уникально с точностью до изометрии.*

Нетрудно заметить, что неприводимый граф G с 13 вершинами удовлетворяет следующим условиям:

1. Степень каждой вершины графа G может быть $0, 3, 4, 5$.

2. Все грани являются выпуклыми многоугольниками с количеством сторон, не превышающим шести.

3. Если $\deg(v) = 0$, $v \in G$, тогда v лежит внутри шестиугольной грани.

4. В шестиугольной грани не может быть двух изолированных (т. е. со степнью 0) точек.

Наше доказательство главной теоремы основано на компьютерном переборе таких сферических неприводимых графов. Мы показываем, что существует всего три возможных неприводимых графа с минимальной дистанцией не меньше чем d_{13}.

Используя сферическую геометрию можно показать, что во всех этих трех случаях мы получаем перноначальный граф. Таким образом, существует единственный (с точностью до изометрии) неприводимый граф, для которого минимальное расстояние соответствующего расположения точек $\approx 57,1367°$. Это завершает доказательство.

О ХРОМАТИЧЕСКИХ ЧИСЛАХ СФЕР В ЕВКЛИДОВЫХ ПРОСТРАНСТВАХ

А. М. Райгородский (Москва)

В середине XX века Э. Нелсон и Г. Хадвигер поставили задачу отыскания *хроматического числа вещественной плоскости* $\mathbb{R}^2$, равного наименьшему количеству цветов, в которые можно так покрасить все точки плоскости, чтобы между одноцветными точками не было расстояния 1. Благодаря работам Хадвигера, П. Эрдеша и М. Гарднера эта задача стала одной из самых известных в комбинаторной геометрии. Общая постановка вопроса выглядит теперь так: *каково минимальное число цветов* $\chi((\Gamma,\rho);\mathcal{A})$, *в которые можно так покрасить все точки метрического пространства* (Γ,ρ), *чтобы расстояние между одноцветными точками не принадлежало множеству различных* (*положительных*) *вещественных чисел* $\mathcal{A}$*?* Искомая величина называется *хроматическим числом метрического пространства* (Γ,ρ) *с множеством запрещенных расстояний* $\mathcal{A}$ (мы запрещаем точкам одного цвета отстоять друг от друга на расстояние из $\mathcal{A}$).

За те десятилетия, что прошли с момента первоначальной постановки проблемы, были написаны сотни работ о хроматических числах различных пространств. Прежде всего изучались [1–4], конечно, пространства $(\mathbb{R}^n, l_p)$ и $(\mathbb{Q}^n, l_p)$, где

$$l_p(\mathbf{x},\mathbf{y}) = \sqrt[p]{|x_1-y_1|^p+\ldots+|x_n-y_n|^p}, \quad p\in[1,\infty),$$

$$l_\infty(\mathbf{x},\mathbf{y}) = \max_{i=1,\ldots,n}|x_i-y_i|,$$

$$\mathbf{x}=(x_1,\ldots,x_n), \qquad \mathbf{y}=(y_1,\ldots,y_n).$$

Даже бесконечные множества запретов не обошли стороной [5].

Еще одно важное направление исследований связано с задачей о хроматических числах сфер $S_r^{n-1}\subset\mathbb{R}^n$, имеющих данный радиус r. В этом случае наиболее интересно поведение величины

$$\chi(S_r^{n-1}) = \chi((S_r^{n-1}, l_2);\{1\}).$$

Иными словами, в качестве запрещенного расстояния здесь берется всего одно число — "классическая" единица. Заметим, что если в случае раскраски всего пространства $\mathbb{R}^n$ величина запрета роли не играла, то здесь она принципиальна. Однако варьировать радиус и всякий раз запрещать расстояние 1 — это в точности то же самое, что и фиксировать радиус, а потом варьировать запрещенное

расстояние. Поэтому хроматические числа $\chi(S_r^{n-1})$ описывают все многообразие возможных ситуаций.

Из работ, посвященных хроматическим числам сфер, стоит отметить статьи Дж. Симмонса [6, 7] о раскрасках сфер в малых размерностях и важную статью Л. Ловаса [8], в которой доказано, что при всех n и при всех $r > \frac{1}{2}$ выполнено $\chi(S_r^n) \geq n+1$. Результат Ловаса, свидетельствующий о том, что хроматическое число любой сферы (кроме тривиальной $S_{1/2}^n$) растет с ростом размерности, получен с помощью топологических методов. Линейная алгебра в комбинаторике позволяет [2, 9] сказать гораздо больше в асимптотике по n.

Теорема 1. *Для любого $r > \frac{1}{2}$ существует такая константа $\gamma > 1$ и такая функция $\delta = \delta(n) = o(1)$, что при всех n выполнена оценка $\chi(S_r^{n-1}) \geq (\gamma + \delta(n))^n$.*

Иными словами, теорема 1 показывает, что при всех r хроматические числа сфер растут экспоненциально. Поскольку $\chi(S_r^{n-1}) \leq \chi((\mathbb{R}^n, l_2); \{1\})$ и известно, что $\chi((\mathbb{R}^n, l_2); \{1\}) \leq (3+o(1))^n$ (см. [10]), мы имеем в итоге точные по порядку верхние и нижние оценки логарифма величины $\chi(S_r^n)$.

Теорема 1 допускает существенное уточнение.

Теорема 2. *Для любого $r \in \left(\frac{1}{2}, \frac{1}{\sqrt{2}}\right)$ существует такая функция $\delta = \delta(n) = o(1)$, что при всех n выполнена оценка*

$$\chi(S_r^{n-1}) \geq \left(2\left(\frac{1}{8r^2}\right)^{\frac{1}{8r^2}}\left(1-\frac{1}{8r^2}\right)^{1-\frac{1}{8r^2}} + \delta(n)\right)^n.$$

Таким образом, при $r \to \frac{1}{\sqrt{2}}$ имеем $\chi(S_r^{n-1}) \geq (1.139... + o(1))^n$, а стало быть, такая же оценка верна и при всех $r \geq \frac{1}{\sqrt{2}}$, ведь, если $r' > r$, то $S_r^{n-1} \subset S_{r'}^n$ и $\chi(S_{r'}^n) \geq \chi(S_r^{n-1})$.

Настоящая работа выполнена при финансовой поддержке гранта РФФИ № 09-01-00294, гранта Президента РФ МД-5414.2008.1, гранта поддержки Ведущих научных школ НШ-691.2008.1, гранта фонда "Династия".

Список литературы

1. Райгородский А. М. Проблема Борсука и хроматические числа некоторых метрических пространств // Успехи матем. наук. — 2001. — 56, № 1. — С. 107–146.

2. Райгородский А. М. Линейно-алгебраический метод в комбинаторике. — М.: МЦНМО, 2007.

3. Székely L. A. Erdös on unit distances and the Szemerédi – Trotter theorems // Paul Erdős and his Mathematics. Bolyai Series Budapest. — J. Bolyai Math. Soc. — Springer, 2002. — V. 11. — С. 649–666.

4. Brass P., Moser W., Pach J., Research problems in discrete geometry. — Springer, 2005.

5. Мощевитин Н. Г., Райгородский А. М. О раскрасках пространства $\mathbf{R}^n$ с несколькими запрещенными расстояниями // Матем. заметки. — 2007. — Т. 81, № 5. — С. 733–744.

6. Simmons G. J. On a problem of Erdős conserning 3-colouring of the unit sphere // Discrete Math. — 1974. — 8. — С. 81–84.

7. Simmons G.J. The chromatic number of the sphere // J. Austral. Math. Soc. Ser. — 1976. — 21. — С. 473–480.

8. Lovaśz L. Self-dual polytopes and the chromatic number of distance graphs on the sphere // Acta Sci. Math. — 1983. — 45. — С. 317–323.

9. Babai L., Frankl P. Linear algebra methods in combinatorics. — Department of Computer Science, The University of Chicago, 1992.

10. Larman D. G., Rogers C. A. The realization of distances within sets in Euclidean space // Mathematika. — 1972. — 19. — С. 1–24.

ДИСТАНЦИОННЫЕ ПОДГРАФЫ ГРАФОВ В ПРОСТРАНСТВАХ МАЛЫХ РАЗМЕРНОСТЕЙ

А. М. Райгородский, М. В. Титова (Москва)

В работе исследуется задача о том, как часто граф с фиксированным количеством вершин содержит индуцированные подграфы, изоморфные дистанционным в пространствах определенных размерностей.

Напомним, что *дистанционным графом в d-мерном евклидовом пространстве* называется граф $G = (V, E)$, в котором множество вершин V является подмножеством пространства $\mathbb{R}^d$, а множество ребер E содержит ребра одинаковой фиксированной длины a (мы будем рассматривать далее только дистанционные графы с $a = 1$). Изучение различных свойств дистанционных графов тесно связано со многими классическими задачами комбинаторной

геометрии, такими, как, например, знаменитая проблема Нелсона—Хадвигера [1, 2]. Если переформулировать ее в терминах дистанционных графов, то речь идет о нахождении хроматического числа $\chi(\mathbb{R}^d)$ дистанционного графа $G = (\mathbb{R}^d, E)$. Согласно теореме Эрдеша—де Брёйна [2], $\chi(G) = \chi(H)$ для некоторого конечного графа $H \subset G$, вследствие чего задачи ставятся об изучении свойств именно конечных дистанционных графов.

В нашем случае мы действуем с точки зрения теории Рамсея. Напомним, что классическим *числом Рамсея* $R(s,t)$ называется такое наименьшее натуральное число, что при любой раскраске ребер полного графа на $R(s,t)$ вершинах в красный и синий цвета имеется либо полный подграф на s вершинах, все ребра которого синие, либо полный подграф на t вершинах, все ребра которого красные [3].

Мы рассматриваем модифицированное число Рамсея $R_{\text{NEH}}(s,t,d)$: под ним мы понимаем минимальное натуральное число n, такое, что для любого графа G на n вершинах либо в G содержится индуцированный подграф на s вершинах, изоморфный некоторому дистанционному графу в $\mathbb{R}^d$, либо в его дополнении $\bar{G}$ содержится индуцированный подграф на t вершинах, изоморфный некоторому дистанционному графу в $\mathbb{R}^d$.

Понятие $R_{\text{NEH}}(s,t,d)$ было введено и исследовано в работе [4], где были получены следующие нижние асимптотические оценки.

Теорема 1. *Выполнено неравенство*

$$R_{\text{NEH}}(s,s,d) \geq R\left(\left[\frac{s}{\chi(\mathbb{R}^d)}\right], \left[\frac{s}{\chi(\mathbb{R}^d)}\right]\right).$$

Теорема 2. *Пусть $s \to \infty$ и $k_0 = k_0(s)$ такое, что*

$$\binom{s}{k_0} 2^{-\binom{k_0}{2}} < 1 < \binom{s}{k_0 - 1} 2^{-\binom{k_0 - 1}{2}};$$

пусть $k_1 = k_0 - 4$. Тогда существует такая функция $\varepsilon(s) = o(1)$ что если соотношение

$$e\left(2\binom{s}{2}\binom{n}{s-2} + 1\right) e^{-\frac{s^2}{2k_1^2}(1+\varepsilon(s))} \leq 1$$

выполнено для n, то для всех $d \leq k_1$ имеем

$$R_{\text{NEH}}(s,s,d) \geq n.$$

Первая из теорем дает лучшую оценку при $d = o(\ln\ln s)$, а при $\ln\ln s = o(d)$ точнее оценка второй теоремы.

Нетрудно заметить из определений, что выполнена верхняя оценка $R_{\mathrm{NEH}}(s,s;d) \le R(s,s)$. В соответствии с оценкой Д. Конлона [5] классического числа Рамсея, лучшая верхняя оценка, которую можно получить, исходя из этого, имеет следующий вид:

$$R_{\mathrm{NEH}}(s,s;d) \le e^{-\gamma\frac{\ln^2 s}{\ln\ln s}} 4^s, \qquad \gamma > 0.$$

Мы получаем новую асимптотическую верхнюю оценку.

Теорема 3. *Выполнено неравенство*

$$R_{\mathrm{NEH}}(s,s;d) \le (d+1) C_{2s-2(d+1)}^{s-(d+1)}.$$

В следующих теоремах мы получаем новые нижние оценки в случае малых размерностей пространства.

Теорема 4. *Пусть $d = 2$. Имеет место оценка*

$$R_{\mathrm{NEH}}(s,s,d) \ge \frac{k}{4\sqrt[4]{2e}}(1+o(1))\, 2^{\frac{k}{8}}, \quad \text{где } k = 0.906s.$$

Теорема 5. *Пусть $d = 3$. Имеет место оценка*

$$R_{\mathrm{NEH}}(s,s,d) \ge \frac{k}{e}(1+o(1))\, 2^{\frac{1}{16}k-\frac{3}{8}}, \quad \text{где } k = \frac{2\pi s}{9}.$$

Методы, с помощью которых доказываются обе теоремы, можно распространить и на более высокие размерности. В теоремах 6 и 7 мы получаем дальнейшие улучшения в размерностях 2 и 3.

Теорема 6. *Пусть $d = 2$. Существует такое $c > 0$, что выполнено неравенство*

$$R_{\mathrm{NEH}}(s,s,d) \ge s(1+o(1))\, e^{\frac{s}{4}-2c\, s^{\frac{1}{3}}}.$$

Теорема 7. *Пусть $d = 3$. Существует такое $c > 0$, что выполнено неравенство*

$$R_{\mathrm{NEH}}(s,s,d) \ge s(1+o(1))\, e^{\frac{s}{4}-2c\, s^{\frac{2}{3}}}.$$

Результаты теорем 6 и 7, в отличие от результатов предыдущих двух теорем, на размерности $d > 3$ не переносятся.

Работа выполнена при финансовой поддержке гранта РФФИ № 09-01-00294, гранта Президента РФ МД-5414.2008.1, гранта поддержки Ведущих научных школ НШ-691.2008.1, гранта фонда "Династия".

Список литературы

1. Райгородский А. М. Линейно-алгебраический метод в комбинаторике. — М.: МЦНМО, 2007.

2. Райгородский А. М. Проблема Борсука и хроматические числа некоторых метрических пространств // Успехи матем. наук. — 2001. — Т. 56. — С. 107–146.

3. Graham R. L., Rothschild B. L., Spencer J. H. Ramsey theory. — NY: John Wiley and Sons, 1975.

4. Райгородский А. М. Об одной серии задач рамсеевского типа в комбинаторной геометрии // Доклады РАН. — 2007. — Т. 413, вып. 2. — С. 171–173.

5. Conlon D. A new upper bound for diagonal Ramsey numbers // To appear in Annals of Maths.

ГЕОМЕТРИЧЕСКИЕ ОБРАЗЫ АВТОМАТОВ И ДИНАМИЧЕСКИЕ СИСТЕМЫ

Л. Б. Тяпаев (Саратов)

Объектами исследования являются геометрические образы автоматов и их преобразования. Определим поведение конечных автоматов геометрическими образами как множествами точек плоскости с рациональными координатами [1–3]. Рассмотрим некоторые преобразования образов и для некоторого класса образов Ω построим динамическую систему $F : \Omega \to \Omega$, в которой функция F будет представлять собой некоторое ортогональное, либо аффинное преобразование.

Пусть X — конечное множество (алфавит). Символом $X*$ мы будем обозначать свободный моноид, порожденный множеством X, элементы которого отождествляются с конечными словами (включая пустое слово e). Множество всех бесконечных слов над алфавитом X вида $x_1x_2x_3...$ обозначим X^ω. Пусть $\xi_1, \xi_2, ..., \xi_n, ...$ — убывающая последовательность положительных чисел ($\lim\limits_{n\to\infty} \xi_n = 0$) и определена метрика в пространстве X^ω $\rho(w_1, w_2) = \xi_n$, где n — длина наибольшего общего начала w_1 и w_2. Расстояние между равными словами полагаем равно 0. На множестве X^ω можно ввести топологию прямого тихоновского произведения конечных дискретных топологических пространств X — топологию поточечной сходимости. В этой топологии X^ω гомеоморфно множеству Кантора. Для

каждого конечного слова $w \in X^*$ множество wX^ω всех слов, начинающихся на w, является в данной топологии открыто-замкнутым, а совокупность всех таких множеств является базой топологии.

Асинхронным автоматом называется набор $A = (S, X, Y, \delta, \lambda, s_0)$, где S— множество состояний, X — входной алфавит, Y— выходной алфавит, $\delta : S \times X \to S$ — функция перехода, $\lambda : S \times X \to Y^*$ — функция выхода, s_0 — начальное состояние. Асинхронный автомат A называется конечным, если S, X, Y — конечные множества. В синхронном автомате функция выхода имеет следующий вид $\lambda : S \times X \to Y$. Отображение $\varphi : X^\omega \to Y^\omega$ определяется автоматом A, если $\varphi(w) = \lambda(s_0, \omega)$ для каждого $w \in X^\omega$. Автоматы, определяющие одно отображение, называются эквивалентными.

Поведение автомата A определяется множеством $\Lambda = \{(p, q) : p \in X^*, q = \lambda(s_0, p)\}$. Пусть $|X| = n$, $|Y| = m$. Геометрическое пространство $\Gamma = \{(\widetilde{x}, \widetilde{y}) : \widetilde{x} \in [0, n+1), \widetilde{y} \in [0, m+1)\}$ для автомата A представляет собой ограниченное подмножество двумерного евклидова пространства. Под геометрическим образом автомата A понимается множество $\Omega(\mathrm{A}) = \{(\widetilde{x}, \widetilde{y}) : (\exists p \in X^*)(\exists q \in Y^*)(\exists c_1, c_2, ..., c_{|p|} \in \{1, 2, ..., n\})(\exists b_1, b_2, ..., b_{|q|} \in \{1, 2, ..., m\})(q = \lambda(s_0, p)) \& \widetilde{x} = \sum_{i=1}^{|p|} \frac{c_i}{(n+1)^{i-1}} \& \widetilde{y} = \sum_{i=1}^{|q|} \frac{b_i}{(m+1)^{i-1}}\}$. Это множество определяет поведение автомата A в пространстве Γ.

Кривая f называется функциональной кривой, если f есть график некоторой непрерывной функции. Отождествим понятие функции, определяющей функциональную кривую, с самой кривой. Функциональная кривая f определяет поведение автомата A в пространстве Γ, если f содержит точки множества $\Omega(\mathrm{A})$. Отметим, что автомат A инициальный. Поведение неинициального автомата в пространстве Γ будет определяться семейством кривых $\{f_s\}_{s \in S}$.

Следующая теорема позволяет получить аналитическое задание геометрических образов автономных синхронных автоматов ($|X| = 1$).

Теорема 1 [4]. *Пусть A автономный автомат,* $|Y| = m$, $|S| = k$. *Тогда поведение автомата A в пространстве* Γ *можно определить функциональной кривой* f, *которая может быть задана следующим уравнением:* $f(\widetilde{x}) = \sum_{j=1}^{m} (j \cdot \sum_{i=1}^{l_j} (m+1)^{\triangle_i{}^{(j)} - \log_2 (2 - \widetilde{x})^{-1}})$, *где* $1 \leq l_j \leq k$, $\triangle_i{}^{(j)} = (k-1) - r_i{}^{(j)}$, $r_i{}^{(j)} \in \{0, 1, ..., k-1\}$.

Пусть даны автоматы A и B. Состояние s автомата A r-остаточно неотличимо от состояния s' автомата B, если для любого

$p \in X^{\geq r}$ выполняется $pr_{r\ldots|p|}(\lambda(s,p)) = pr_{r\ldots|p|}(\lambda(s',p))$. Неотличимость состояний в этом смысле обозначим $s \approx s'$. Предположим, что для любого состояния s автомата A существует r-остаточно неотличимое состояние s' автомата B, и обратно, для любого s' существует r-остаточно неотличимое состояние s. Говорим в указанной ситуации, что автоматы A и B r-остаточно неотличимы. Неотличимость автоматов A и B обозначим $A \overset{r}{\approx} B$.

Теорема 2 [2]. *Пусть* $\{f_s\}_{s\in S_A}$, $\{g_s\}_{s\in S_B}$ — *кривые, определяющие поведение автоматов* A *и* B *в пространстве* Γ. *Если для любой кривой* f_s *существует конгруэнтная в* Γ *кривая* g_s, *и обратно, для любой кривой* g_s *существует конгруэнтная кривая* f_s, *то* $A \overset{2}{\approx} B$.

Пусть f, f' — некоторые кривые, которые определены в пространстве Γ и задают поведение некоторых автоматов A и A$'$ в этом пространстве. Пусть f' есть образ f при некотором ортогональном (аффинном) преобразовании φ. Тогда автомат A$'$ назовем образом автомата A при преобразовании φ.

Теорема 3. *Для любого конечного синхронного автомата* A *существует образ аффинного преобразования конечный асинхронный автомат* B.

Динамическая система определяется множеством геометрических образов автоматов и набором ортогональных, либо аффинных преобразований. Конгруэнтность (аффинная эквивалентность) образов порождает разбиение множества образов на классы эквивалентности, что приводит к разбиению фазового пространства динамической системы на компоненты связности. Для некоторого класса выделенных геометрических образов найден минимальный по числу образов базис [5].

Список литературы

1. Тяпаев Л. Б. О задании конечных автоматов функциями, определенными на открытом промежутке // Проблемы и перспективы прецизионной механики и управления в машиностроении. Материалы Междунар. конф. — Саратов, 1997. — С. 48–49.

2. Тяпаев Л. Б. Геометрическая модель поведения автоматов и их неотличимость // Математика. Механика. Математическая кибернетика. Сб. науч. тр. — Саратов: Изд-во Сарат. ун-та, 1999. — С. 139–143.

3. Тяпаев Л. Б. Геометрические образы автоматов как множества точек плоскости с рациональными координатами // Автоматизация проектирования дискретных систем (CAD DD'2001). Материалы IV Межд. конф. — Минск, Институт технической кибернетики НАН Беларуси, 2001. — С. 203–210.

4. Тяпаев Л. Б. Решение некоторых задач для конечных автоматов на основе анализа их поведения // Изв. Сарат. ун-та. Сер. Математика. Механика. Информатика. — 2006. — Т. 6, вып. 2. — С. 121–133.

5. Тяпаев Л. Б., Матов Д. О. Базисы геометрических образов для динамических систем, определяемых некоторыми классами автоматов // Компьютерные науки и информационные технологии. Материалы Межд. конф. — Саратов, 2009. — С. 201–204.

Секция
«Теория кодирования и математические вопросы теории защиты информации»

О ПРИБЛИЖЕНИИ БУЛЕВЫХ ФУНКЦИЙ ПОЧТИ ЛИНЕЙНЫМИ ФУНКЦИЯМИ

В. Б. Алексеев, Р. Р. Омаров (Москва)

Булевы функции широко применяются в криптографии, и стойкость систем шифрования часто основывается на «сложности» используемых булевых функций. Поскольку аффинные функции считаются простыми, то в качестве одной из характеристик «сложности» булевых функций рассматривают «удаленность» данной функции от всех аффинных функций. Этому параметру, называемому *нелинейностью* булевой функции, посвящено множество работ. Обзор имеющихся результатов о нелинейности (с указанием имеющихся публикаций) можно найти в книге [1], где нелинейности посвящена отдельная глава. Дадим необходимые определения.

Пусть n — любое натуральное число. Через V_n будем обозначать векторное пространство наборов длины n с компонентами из $\{0,1\}$ с операцией $\oplus$ покоординатного сложения векторов по модулю 2.

Определение. Пусть f, g — булевы функции от n переменных, то есть $f : V_n \to \{0,1\}$ и $g : V_n \to \{0,1\}$. *Расстояние* $dist(f,g)$ от булевой функции f до булевой функции g определяется как число наборов, на которых значения функций f и g различаются.

Определение. Пусть f — булева функция от n переменных и M — произвольное множество булевых функций от n переменных. *Расстоянием от f до множества M* называется величина $dist(f,M) = \min_{g\in M} dist(f,g)$.

Определение. Пусть $x \in V_n$, $y \in V_n$. Через $\langle x,y\rangle$ будем обозначать *скалярное произведение* x и y: $\langle x,y\rangle = x_1y_1 \oplus \ldots \oplus x_ny_n$ (здесь $\oplus$ — это сложение по модулю 2).

Определение. Булева функция f от n переменных называется *аффинной*, если существуют $a = (a_1,\ldots,a_n) \in V_n$ и $c \in \{0,1\}$ такие, что $g(x) = \langle a,x\rangle \oplus c = a_1x_1 \oplus \ldots \oplus a_nx_n \oplus c$. Множество всех аффинных булевых функций от n переменных будем обозначать A_n.

Определение. Расстояние $dist(f, A_n)$ от булевой функции $f(x)$ от n переменных до множества A_n аффинных булевых функций называется *нелинейностью* функции $f(x)$ и обозначается через N_f.

Лемма 1 [1]. *Для любой булевой функции $f(x)$ от n переменных справедливо неравенство $N_f \leq 2^{n-1} - 2^{n/2-1}$. Для четных n эта оценка достижима.*

Определение. Булевы функции $f(x)$ от $2n$ переменных, для которых $N_f = 2^{2n-1} - 2^{n-1}$, называют *максимально-нелинейными* функциями (этот класс называют также классом *бент-функций*).

Определение. Пусть $x = (x_1, \ldots, x_n)$, $y = (y_1, \ldots, y_n)$. *Класс Мэйорана—Мак-Фарланда* определяется как множество всех булевых функций $f(x, y)$ от $2n$ переменных вида $f(x, y) = \langle \pi(y), x \rangle \oplus \Phi(y)$, где π — произвольная подстановка на множестве V_n, а $\Phi(y)$ — произвольная булева функция от n переменных.

Лемма 2 [1]. *Все функции из класса Мэйорана—Мак-Фарланда являются максимально-нелинейными, то есть для любой функции f от $2n$ переменных из этого класса выполняется равенство $dist(f, A_{2n}) = 2^{2n-1} - 2^{n-1}$.*

В статье [2] мы исследовали вопрос о том, что происходит с расстоянием до класса приближающих функций, если этот класс немного расширяется.

Определение. Через AE_n будем обозначать класс всех почти аффинных функций $g(x)$ от n переменных, а именно, функций вида $g(x) = \langle a, x \rangle \oplus c \oplus x_{i_1} \cdot \ldots \cdot x_{i_k}$, где $a \in V_n$, $c \in \{0, 1\}$ и $\{i_1, \ldots, i_k\}$ — произвольное подмножество (возможно, пустое) множества $\{1, \ldots, n\}$.

Оказывается, что при переходе от класса A_{2n} к классу AE_{2n} для всех функций из класса Мэйорана–Мак-Фарланда расстояние до класса уменьшается, причем по-разному (то есть в классе Мэйорана—Мак-Фарланда есть "более стойкие" и "менее стойкие" функции). А именно, в статье [2] нами доказана следующая теорема.

Теорема 1 [2]. *Для всех функций $f(x, y) = \langle \pi(y), x \rangle \oplus \Phi(y)$ из класса Мэйорана–Мак-Фарланда от $2n$ переменных при всех $n \geq 2$ выполняются неравенства:*

$$2^{2n-1} - 3 \cdot 2^{n-1} + 2 \leq dist(f, AE_{2n}) \leq 2^{2n-1} - 2 \cdot 2^{n-1},$$

причем обе границы достижимы (при $n = 1$ $dist(f, AE_{2n}) = 0$ для всех f).

Легко заметить, что, в отличие от класса A_n, класс AE_n не является замкнутым относительно невырожденных афинных преобразований. Поэтому больший интерес представляет исследование расстояния от функций класса Мэйорана—Мак-Фарланда до класса,

содержащего все функции из AE_n, а таже все функции, аффинно эквивалентные им. В частности, интересно, сохраняются ли полученные для AE_n оценки?

Определение. Через $\widetilde{AE}_n$ будем обозначать класс всех функций, аффинно эквивалентных функциям из класса AE_n, а именно, функций вида $g(Ax \oplus d)$, где $g \in AE_n$, $A = (a_{ij})$ — произвольная невырожденная матрица размера $n \times n$, причем $a_{ij} \in \{0, 1\}$, а $d \in V_n$ — произвольный вектор.

Так как $AE_n \subseteq \widetilde{AE}_n$, то для любой булевой функции от n переменных выполняется неравенство

$$dist(f, \widetilde{AE}_n) \leq dist(f, AE_n).$$

Оказывается, что переход от класса AE_{2n} к классу $\widetilde{AE}_{2n}$ не изменяет оценок, приведенных в теореме 1. А именно, верна следующая теорема.

Теорема 2. *Для всех функций $f(x, y) = \langle \pi(y), x \rangle \oplus \Phi(y)$ из класса Мэйорана—Мак-Фарланда от $2n$ переменных при всех $n \geq 2$ выполняются неравенства:*

$$2^{2n-1} - 3 \cdot 2^{n-1} + 2 \leq dist(f, \widetilde{AE}_{2n}) \leq 2^{2n-1} - 2 \cdot 2^{n-1},$$

причем обе границы достижимы (при $n = 1$ $dist(f, \widetilde{AE}_{2n}) = 0$ для всех f).

Так как класс $\widetilde{AE}_{2n}$ инвариантен относительно аффинных преобразований, то справедливо следующее утверждение.

Следствие. *Утверждение теоремы 2 верно и для класса всех функций, аффинно эквивалентных функциям из класса Мэйорана–Мак-Фарланда (все они являются максимально-нелинейными).*

Работа выполнена при финансовой поддержке РФФИ (проекты 09-01-00701-а и 10-01-00475-а).

Список литературы

1. Логачёв О. А., Сальников А. А., Ященко В. В. Булевы функции в теории кодирования и криптологии. — М.: Изд-во МЦНМО, 2004.

2. Алексеев В. Б., Омаров Р. Р. Исследование одного параметра булевых функций, близкого к нелинейности // Научные ведомости Белгородского университета. Серия "Информатика". — В печати.

ОТОБРАЖЕНИЯ КЛОСТЕРМАНА—ХАССЕ И ИХ КОДИРОВАНИЕ

Н. М. Глазунов (Киев)

В книге [1] представлены и исследованы функции, определенные на целых числах, на классах вычетов по простым модулям со значениями в единичном интервале, а также рассмотрены некоторые вопросы кодирования числовых последовательностей бесконечными в одну сторону последовательностями. Мы строим отображения в квадрат $[0,\pi]\times[0,\pi]$ и кодируем их продолжающимися (в том числе и бесконечными) в обе стороны последовательностями. Определяются отображения, которые мы называем отображениями Клостермана—Хассе (КХ). Отображения строятся на основе сумм Клостермана и кубических кривых. Мы определяем функциональное и арифметическое отображения Клостермана—Хассе. Определяется и исследуется целочисленное кодирование отображений КХ на основе прямого произведения конечных равномощных разбиений интервала $[0,\pi]$, и интерпретация этого кодирования точками единичного квадрата.

Пусть $\mathbf{F}_p$ есть простое конечное поле, $\mathbf{F}_p^*$ — мультипликативная группа поля $\mathbf{F}_p$, $Spec\,\mathbf{Z}$ — аффинная схема над кольцом целых чисел $\mathbf{Z}$, d_1 — множество точек, в которых $c,d\equiv 0 \bmod p$, $Sp = Spec\mathbf{Z}\setminus d_1$.

Определим *функциональное отображение КХ.*

Компонента Хассе. Пусть $y^2 = f(x)$, $f(x) = x^3 + cx + d$, есть кубический многочлен в простом конечном поле $\mathbf{F}_p$. Для числа $\#C_p$ решений кривой $C : y^2 = f(x)$ в $\mathbf{F}_p$ имеет место формула $\#C_p = \sum_{x=0}^{p-1}\left(1+\left(\frac{f(x)}{p}\right)\right)$, где $\left(\frac{f(x_0)}{p}\right)$ есть символ Лежандра с числителем, равным значению многочлена $f(x_0)$ в точке $x_0\in\mathbf{F}_p$. Легко видеть, что $\#C_p = p - a_p$, где $a_p = -\sum_{x=0}^{p-1}\left(\frac{f(x)}{p}\right)$. Если C есть эллиптическая кривая, то число точек $\#C(\mathbf{F}_p)$ кривой C выражается формулой $\#C_p = 1 + p - a_p$, где $a_p = 2\sqrt{p}\cos\varphi_p$, а сама кривая C рассматривается как проективная. Если C не есть эллиптическая кривая, то значение a_p равно 1, -1 или 0 и легко вычисляется [2]. В обоих случаях вычисляем:$\varphi_p = \arccos(a_p/2\sqrt{p})$ и приводим его к интервалу $[0,\pi]$. Гипотеза Сато—Тэйта (в функциональном случае это теорема Б. Берча [3]) утверждает, что для эллиптических кривых без комплексных умножений углы φ_p, соответствующие a_p, равнораспределены на интервале $[0,\pi]$ с плотностью $(2/\pi)\sin^2 t$.

Компонента Клостермана. Пусть cd не сравнимо с нулем по $\bmod p$, $T_p(c,d) = \sum_{x=1}^{p-1} e^{2\pi i(\frac{cx+\frac{d}{x}}{p})}$ есть сумма Клостермана. Согласно

А. Вейлю [4], $T_p(c,d) = 2\sqrt{p}\cos\theta_p(c,d)$. Последовательно вычисляем $T_p, \cos\theta_p, \theta_p$ и приводим θ_p к интервалу $[0,\pi]$. В функциональном случае теорема Делиня-Каца-Адольфсона [4] утверждает, что углы θ_p равнораспределены на интервале $[0,\pi]$ с плотностью $(2/\pi)\sin^2 t$. Экспериментальное исследование распределения углов сумм Клостермана в функциональном случае представлено в работе [5].

Отображение Клостермана—Хассе. Функциональное отображение КХ определяется на $\mathbf{F}_p^* \times \mathbf{F}_p^*$ со значениями в $\Pi = [0,\pi]\times[0,\pi]$ и имеет вид $hk(c,d) = (\varphi_p(c,d), \theta_p(c,d))$. Так как c, d независимо пробегают мультипликативную группу $\mathbf{F}_p^*$, их произведение не может делиться на p, и тем самым отображение $hk(c,d)$ определено во всех точках.

Кодирование. Пусть $\mathcal{R}_1$ и $\mathcal{R}_2$ есть два конечных разбиения одинаковой мощности d интервала $[0,\pi]$. Будем называть $\mathcal{R}_1$ горизонтальным, а $\mathcal{R}_2$ вертикальным разбиениями сторон квадрата $\Pi = [0,\pi]\times[0,\pi]$, а саму пару разбиений $\mathcal{R}_1, \mathcal{R}_2$ p-парой. Обозначим элементы разбиений целыми числами $0, 1, \ldots, d-1$. Функциональное отображение КХ кодируется конечной последовательностью $(b_s b_{s-1}\ldots b_1 b_0.a_1 a_2 \ldots a_r)$. Значение этой последовательности может быть интерпретировано как рациональное число (x,y) из единичного квадрата, если известным способом полагать, что $x = \sum_{i=1}^{r} a_i/d^i$ (соответственно, $y = \sum_{i=1}^{s} b_{i-1}/d^i$ есть $d-$ичное разложение x (соответственно y).

Определим *арифметическое отображение КХ.*

Компонента Хассе. Если C есть эллиптическая кривая над $\mathbf{Z}$, то вне конечного множества простых, являющихся делителями дискриминанта, кривая C имеет хорошую редукцию в поле $\mathbf{F}_p$. Число точек $\#C(\mathbf{F}_p)$ кривой C при локализации по $\bmod p$ выражается формулой $\#C_p = 1 + p - a_p$, где $a_p = 2\sqrt{p}\cos\varphi_p$, а сама кривая C рассматривается как проективная. Если локализация C в поле $\mathbf{F}_p$ не есть эллиптическая кривая, то значение a_p равно 1, -1 или 0 и легко вычисляется [2]. В обоих случаях вычисляем:$\varphi_p = \arccos(a_p/2\sqrt{p})$ и приводим его к интервалу $[0,\pi]$.

Компонента Клостермана. Пусть cd не сравнимо с нулем по $\bmod p$, $T_p(c,d) = \sum_{x=1}^{p-1} e^{2\pi i(\frac{cx+\frac{d}{x}}{p})}$ есть сумма Клостермана. Согласно А. Вейлю [4], $T_p(c,d) = 2\sqrt{p}\cos\theta_p(c,d)$. Последовательно вычисляем $T_p, \cos\theta_p, \theta_p$ и приводим θ_p к интервалу $[0,\pi]$. Экспериментальное исследование распределения углов сумм Клостермана в арифметическом случае представлено в работе [5].

Отображение Клостермана—Хассе. Арифметическое отображение КХ определяется на произведении схем $Sp \times Sp$ со значениями в П и имеет вид $hk(c,d) = (\varphi_p(c,d), \theta_p(c,d))$. Так как Sp не содержит, по построению, простых делителей cd, отображение $hk(c,d)$ определено во всех точках. В проведенном экспериментальном исследовании [5] с суммой Клостермана $T_p = T_p(1,1)$ схема Sp совпадает с $Spec\,\mathbf{Z}$.

Кодирование. Определение p-пары и обозначение элементов разбиения аналогично функциональному случаю. Арифметическое отображение КХ кодируется бесконечной последовательностью $(\ldots b_1 b_0.a_1 a_2 \ldots)$. Значение этой последовательности может быть интерпретировано как вещественное число (x,y) из единичного квадрата, если известным способом полагать, что $x = \sum_{i=1}^{\infty} a_i/d^i$ (соответственно, $y = \sum_{i=1}^{\infty} b_{i-1}/d^i$) есть $d-$ичное разложение x (соответственно y).

Замечание. Числа $x = \sum_{i=1}^{\infty} a_i/d^i$ (соответственно, $y = \sum_{i=1}^{\infty} b_{i-1}/d^i$) естественно назвать числами Клостермана (соответственно, Хассе) и поставить вопрос — каковы арифметические свойства этих чисел?

Рассмотрим арифметическое отображение КХ и заданную p-пару. Отображению $hk(c,d)$ и его кодированию посредством заданной p-пары соответствует двусторонний сдвиг

$$\sigma(\ldots b_1 b_0.a_1 a_2 \ldots) = \ldots b_1 b_0 a_1.a_2 \ldots,$$

где $a_1 a_2 \ldots$ соответственно $b_0 b_1 \ldots$ определены выше.

Список литературы

1. Постников А. Г. Избранные труды. — М.: Физматлит, 2005. — С. 18–147.

2. Постникова Л. П. Тригонометрические суммы и теория сравнений по простому модулю. — М.: МГПИ, 1973.

3. Birch B. How the number of points of an elliptic curve over a fixed prime field varies // Journ. London Math. Soc. — 1968. — 43. — P. 57–60.

4. Katz N. M. Gauss sums, Kloosterman sums, and monodromy groups. — Princeton: Princeton Univ. Press, 1988.

5. Глазунов Н. М. Методы обоснования арифметических гипотез и компьютерная алгебра // Программирование. — 2006. — № 3. — С. 10–16.

О ПЕРЕСТАНОВКАХ НА ОСНОВЕ ЛИНЕЙНЫХ ПРЕОБРАЗОВАНИЙ

М. В. Карташова (Москва)

Рассматриваются вопросы реализации нелинейных псевдослучайных перестановок с неоднократным использованием линейных преобразований

Псевдослучайные перестановки (ПСПР) используются, например, в криптографии.

Рассмотрим реализацию нелинейных ПСПР с использованием линейных преобразований

$$y = ax + b \pmod{m}.$$

Вначале рассмотрим наиболее простой случай.

Выбираем модуль m и числа a_1, b_1, a_2, b_2, удовлетворяющие условиям одноцикловости линейных преобразований

$$y = a_1x + b_1 \pmod{m}, \quad y = a_2x + b_2 \pmod{m}.$$

Выбираем числа c_0^1 и c_0^2 и строим ЛПММП [1] C_1 и C_2^1 , являющиеся (m, a_1, b_1, c_0^1)- и (m, a_2, b_2, c_0^2)-ЛПММП, соответственно. Определения приведены в работе Орлова В.А. и Карташовой М.В. настоящего сборника.

Каждый элемент ПСП [1] C_2^1 увеличиваем на m. Полученную таким образом ПСП обозначим через C_2. Выбираем одноцикловую перестановку

$$h(x) = a_3x + b_3 \pmod{m}$$

и строим $(2m, a_3, b_3, c_0^3)$-ЛПММП C_4.

Последовательность C_3, являющуюся конкатенацией C_1 и C_2, переставляем в соответствии с ЛПММП C_4.

Нетрудно убедиться в том, что полученная таким способом ПСП C_5 не является линейной. Этой ПСП соответствует нелинейная перестановка $2m$ элементов.

Отметим недостаток этой ПСП. Зная C_5, нетрудно найти ЛПММП C_4. Для устранения этого недостатка разработана модификация построения последовательности C_3.

Предложенный подход нетрудно обобщить на случай конкатенации нескольких ЛПММП с различными периодами и разными (регулярными) способами увеличения значений элементов этих ЛПММП.

Такие ПСП будем называть 1-НЛП. Если элементами конкатенаций являются 1-НЛП, то получим ПСП, которые будем называть 2-НЛП. Этот процесс можем повторять несколько раз.

Таким образом, предложены подходы к реализации нелинейных ПСП и перестановок большой длины, имеющих небольшую длину ключа.

Список литературы

1. Орлов В. А., Карташова М. В. О реализации псевдослучайных перестановок и последовательностей с использованием линейных преобразований // Информационные технологии управления в социально-экономических системах. — 2009. — № 3. — С. 87–91.

ИДЕАЛЬНЫЕ МОДУЛЯРНЫЕ СХЕМЫ РАЗДЕЛЕНИЯ СЕКРЕТА

Г. В. Матвеев, Н. Н. Шенец (Минск)

Модулярные схемы разделения секрета были предложены Миньоттом [1], Асмусом и Блюмом [2]. Они основаны на решении системы сравнений в кольце целых чисел. Пусть $I = \{1, 2, \ldots, t\}$ — множество участников, а число c — *секрет*. Каждый участник $i \in I$ располагает натуральным модулем m_i и числом $s_i = c \pmod{m_i}$ — наименьшим неотрицательным вычетом секрета c по модулю m_i, которое называется *частичным секретом* участника. Тогда любое подмножество участников $A \subseteq I$ находит значение c, решая соответствующую систему сравнений. Однако правильно найдут секрет лишь те подмножества участников A, для которых выполнено условие $c < \text{НОК}[m_i, i \in A]$. Асмус и Блюм предложили приводить секрет c по дополнительному модулю m_0, что позволяет приблизить его размер к размерам частичных секретов.

С разделением секрета тесным образом связано понятие *структуры доступа*, под которой понимается семейство подмножеств Γ множества участников I, обладающее свойством монотонности, т. е. $A \in \Gamma, A \subseteq B \subseteq I \Rightarrow B \in \Gamma$. Подмножества из семейства Γ называются разрешенными. Все остальные подмножества называются запрещенными. Они образуют структуру отказа $\overline{\Gamma}$. Любая структура доступа задается набором своих минимальных по включению подмножеств $\Gamma_{\min}$, а структура отказа — максимальным по включению набором $\overline{\Gamma}_{\max}$.

Важным частным случаем структуры доступа является (k,t)-пороговая структура доступа. Здесь разрешенным будет всякое подмножество A, если $|A| \geq k$, для некоторого k, $1 \leq k \leq t$.

В дальнейшем модулярный подход был развит в работах [3, 4]. Он был обобщен на случай кольца полиномов $\mathbb{F}_q[x]$ над полем Галуа $\mathbb{F}_q$. Было показано, что любая структура доступа допускает модулярную реализацию в кольцах целых чисел и полиномов над полями Галуа. Получен также ответ на известный вопрос о том, какие структуры доступа могут быть реализованы с помощью попарно взаимно простых модулей. Такие структуры доступа были названы *элементарными*, они могут быть заданы с помощью линейной формы.

При построении схем разделения секрета стараются удовлетворить нескольким естественным требованиям. К их числу относится требование *совершенности*, т.е. чтобы запрещенные множества участников не получали никакой дополнительной информации к имеющейся априорной о возможном значении секрета c. Для таких схем вводится понятие *информационного уровня* ρ, который равен минимуму отношения размера сектрета к размерам частичных секретов. Известно, что $0 < \rho \leq 1$. В случае $\rho = 1$ схема называется *идеальной*. Формальные определения имеются в работе [5].

В настоящий момент для модулярных схем разделения секрета известно мало результатов, связанных с оценками их качества. Так в работе [5] была построена асимптотически совершенная и асимптотически идеальная пороговая схема над кольцом целых чисел при $m_0 \to \infty$. Отметим, что в этом кольце вообще нельзя построить совершенную модулярную схему разделения секрета. Переход же к кольцу полиномов над полем Галуа позволил преодолеть это препятствие, и в работе [4] была предложена совершенная и идеальная реализация пороговой структуры доступа. Однако для других структур доступа никаких оценок качества их модулярных реализаций до настоящего момента получено не было.

Пусть $m_1(x), m_2(x), \ldots, m_t(x) \in \mathbb{F}_q[x]$ — модули участников. Для реализации структуры доступа Γ необходимо и достаточно, чтобы выполнялось условие:

$$M_1 = \deg \max_{A \in \overline{\Gamma}} \text{НОК}[m_i(x), i \in A] < \deg \min_{A \in \Gamma} \text{НОК}[m_i(x), i \in A] = M_2.$$

Рассмотрим схему Асмуса—Блюма. Пусть $m_0(x)$ — дополнительный модуль. Тогда секрет $c(x)$ случайным образом выбирается на множестве полиномов, степень которых меньше $\deg m_0(x)$. Затем случайным образом генерируется полином $p(x)$, степень которого

меньше $M_2 - \deg m_0(x)$. В результате формируется промежуточное значение секрета $C(x) = m_0(x)p(x) + c(x)$, $\deg C(x) < M_2$. Отметим, что все значения полинома $C(x)$ равновероятны. Частичный секрет i-го участника вычисляется по формуле $s_i(x) = C(x) \pmod{m_i(x)}$.

Теорема 1. *Реализация схемы Асмуса—Блюма в кольце полиномов над полем Галуа будет совершенной тогда и только тогда, когда*:

1. НОД$(m_0(x), m_i(x)) = 1$, $\forall i \in I$.

2. $\deg m_0(x) \leq M_2 - M_1$.

Определение. Два участника i и j из множества I называются *взаимозаменяемыми*, если для любого подмножества $A \in \overline{\Gamma}_{max}$ справедливо $i \in A \Leftrightarrow j \in A$.

Взаимозаменяемым участникам можно давать одинаковые модули. При этом без потерь можно рассматривать ту же структуру доступа, заменив взаимозаменяемых участников одним участником. Поэтому мы рассматриваем структуры доступа без таких участников.

Теорема 2. *Идеальной модулярной реализацией в кольце полиномов над полем Галуа обладает только пороговая структура доступа.*

Теорема 3. *В классе элементарных непороговых структур доступа оптимальный информационный уровень равен* $1/2$. *Он достигается на структурах, задаваемых линейными формами с коэффициентами* 1 *и* 2.

Список литературы

1. Mignotte M. How to share a secret // Lecture Notes in Computer Science. Advances in cryptology (Eurocrypt'82). — 1983. — P. 371–375.

2. Asmuth C. A., Bloom J. A modular approach to key safeguarding // IEEE Transactions on Information Theory. — 1983. — V. 29. — P. 208–210.

3. Galibus T., Matveev G. Generalized Mignotte sequences in polynomial rings // Electronic Notes in Theoretical Computer Science. — 2007. — V. 186. — P. 41–46.

4. Galibus T., Matveev G., Shenets N. Some structural and security properties of the modular secret sharing // SYNASC'08. — LosAlamitos (California): IEEE Comp. Soc. Press, CPS, 2009. — P. 197–200.

5. Quisquater M., Preneel B., Vandewalle J. On the security of the threshold scheme based on the Chinese remainder theorem // Lecture Notes in Computer Science. — 2002. — V. 2274. — P. 199–210.

О МУЛЬТИЛИНЕЙНЫХ ПЕРЕСТАНОВКАХ

В. А. Орлов, М. В. Карташова (Москва)

Рассматриваются вопросы реализации нелинейных псевдослучайных перестановок с неоднократным использованием линейных преобразований.

Псевдослучайные перестановки (ПСПР) используются в различных приложениях. В частности, их используют в криптографии в шифрах простой замены, перестановки и гаммирования.

Представляет интерес получение перестановок большой мощности с малой длиной ключа. Одним из таких способов является использование преобразования

$$y = ax + b \pmod{m},$$

которое называют *линейным*. Это преобразование взаимнооднозначно тогда и только тогда, когда числа a и m являются взаимно простыми.

Пусть для простоты $m = 2^k$. Запись перестановки имеет $k2^k$ бит. Длина ключа $3k$ бит (запись чисел m, a и b). Таким образом, имеем хорошее соотношение между мощностью перестановки и длиной ключа.

При построении псевдослучайных последовательностей (ПСП) предпочтение отдают перестановкам, имеющим один цикл.

Известен следующий критерий одноцикловости линейной перестановки.

Пусть $m = 2^{s_1}p_2^{s_2}...p_k^{s_k}$. Линейная перестановка $y = ax+b \pmod{m}$ является одноцикловой тогда и только тогда, когда: 1) $НОД(a, m) = НОД(b, m) = 1$; 2) Если $0 \le s_1 \le 1$, то $a \equiv 1 \pmod{p_2...p_k}$; 3) Если $s_1 \ge 2$, то $a \equiv 1 \pmod{4p_2...p_k}$.

На основе линейного преобразования ПСП $C = c_0, c_1, ..., c_n, ...$ получают следующим способом.

Выбирают c_0, $0 \le c_0 \le m-1$. Затем c_i, $i > 0$ полагают равным $ac^{i-1} \pmod{m}$.

Если преобразование $y = ax + b \pmod{m}$ является одноцикловой перестановкой, то ПСП имеет период максимально возможной длины m. ПСП с начальным значением c_0, полученную таким способом из одноцикловой перестановки $y = ax + b \pmod{m}$, будем называть (m, a, b, c_0)-ЛПМП (линейной ПСП максимального периода).

Замечание. Из критерия одноцикловости следует, что если модуль m является числом свободным от квадратов, то $a \equiv 1 \pmod{m}$ и ЛПМП является тривиальной и имеет вид $0, b, 2b, ..., (m-1)b$.

ЛПМП легко реализовать, но, зная модуль m и три ее последовательные элемента легко вычислить параметры a и b, т. е. всю последовательность.

Отметим, что суперпозиция (произведение) линейных перестановок является линейной перестановкой. Однако суперпозиция линейных одноцикловых перестановок может не быть одноцикловой перестановкой.

Кажется перспективным построение ПСП перестановкой элементов ЛПМП C_1 в соответствии с (m, a_2, b_2, h_0)-ЛПМП $H = h(0), h(1), ..., h(m-1)$, т. е. получение ПСП $C_2 = c_{h(0)}, c_{h(1)}, ..., c_{h(m-1)}$.

Как оказалось, к такому построению ПСП следует подходить с осторожностью. А именно, получены необходимые и достаточные условия, при которых ПСП C_2 является нелинейной.

Теорема 1. *Пусть* $P_1 = c_0, c_1, ..., c_{m-1}$ — (m, a_1, b_1, c_0)-*ЛПМП, пусть* $h(x) = a_2 x + b_2 \pmod m$ *и пусть* $P_2 = c_{h(0)}, c_{h(1)}, c_{h(m-1)}$. *Тогда для любых* a_2 *и* b_2 *таких, что НОД*$(a_2, m) = 1$, P_2 *является* $(m, a_1^{a_2}, c_{a_2})$-*ЛПМП.*

С использованием предложенного авторами метода геометрических сумм доказано следующее утверждение.

Теорема 2. *Пусть* $m = p_1^{t_1}, p_2^{t_2} \cdot p_n^{t_n}$, $P_1 = c_0, c_1, ..., c_{m-1}$, — (m, a_1, b_1, c_0)-*ЛПМП,* $H = h(0), h(1), ..., h(m-1)$ — $m, a_2, b_2, h(0)$-*ЛПМП и пусть* $P_2 = c_{h(0)}, c_{h(1)}, ..., c_{h(m-1)}$. *Пусть для любого* j, $1 \le j \le n$ $a_1 \equiv 1 \pmod{p_j^{u_j}}$, $a_2 \equiv 1 \pmod{p_j^{v_j}}$ *и* $u_j + v_j \ge t_j$. *Тогда* P_2 *является* $(m, a_1^{a_2}, c_{a_2}, c_{b_2})$-*ЛПМП.*

При невыполнении условий теоремы 2 последовательность P_2 не является ЛПМП.

Работа выполнена при частичной финансовой поддержке РФФИ (проект 08–01–00863).

Список литературы

1. Орлов В. А., Карташова М. В. О псевдослучайных последовательностях на основе линейных преобразований // Безопасность информационных технологий. — 2009. — № 3. — С. 53–55.

ОДНО ОБОБЩЕНИЕ ЛИНЕЙНЫХ СТРУКТУР

Б. А. Погорелов, М. А. Пудовкина (Москва)

Линейная структура отображений (блочных шифрсистем) рассматривалась в работах [1–4] и др. Наличие нетривиальной линейной структуры является слабостью криптографического отображения, в частности, позволяет применять методы гомоморфизмов, разностный или линейный. В данной работе рассматриваются фактор-структуры преобразований, являющиеся непосредственным обобщением линейных структур. Также показывается их связь с разностями высших порядков.

Будем придерживаться следующих обозначений: $\mathbb{N}_0$ — множество натуральных чисел с нулем; $m \in \mathbb{N}_0$, $m \geq 2$; R — конечное коммутативное кольцо с единицей; p — простое число; $\overline{a,b} = a, a+1, ..., b, a < b$; $S(X)$ — симметрическая группа на множестве X; H — конечная аддитивная группа или R-модуль, чаще всего $H \in \{GF(p^m), V_m(p), \mathbb{Z}_{p^m}\}$, $S_d = S(X)$ при $|X| = d$; $\vec{0}$ — нулевой элемент H, $G_1 \int G_2$ — сплетение групп подстановок G_1, G_2.

Напомним (см., например, [5]), что преобразование $\pi \in S(H)$ обладает линейной структурой, если в аддитивной группе H существует ненулевой элемент α такой, что $(\beta+\alpha)^\pi = \beta^\pi + \gamma_\alpha$ для любого $\beta \in H$, где γ_α — некоторый фиксированный ненулевой элемент из H. Элемент α называется линейным транслятором отображения π.

Пусть

$$\Pi_{W,X} = \{\pi \in S(H) | (\beta + W)^\pi = \beta^\pi + X, \forall \beta \in H\},$$

где W, X — непустые подмножества H одинаковой мощности.

Будем говорить, что преобразование $\pi \in S(H)$ обладает фактор-структурой, если в H существуют такие непустые подмножества $W, X \subset H$, $|W| = |X|$, что $(\beta + W)^\pi = \beta^\pi + X$ для любого $\beta \in H$. Наличие фактор-структуры может привести, например, к применению метода гомоморфизмов.

Утверждение 1. *Пусть $(H, +)$ — произвольная конечная группа, W — её произвольная нетривиальная подгруппа, $|H| = b$, $|W| = d$. Пусть также X — такое подмножество H, что существует отображение $g \in S(H)$, удовлетворяющее соотношениям: $W^g = X$ и $(\beta + W)^g = \beta^g + X$ для всех $\beta \in H$. Тогда* 1. *X — подгруппа группы H.*

2. $\Pi_{W,X} = \Pi_{W,W} g = (S_d \int S_{d^{-1}b})\, g$.

Следствие 2. *Пусть* $(H,+)$ *— конечная группа,* W *— её произвольная нетривиальная подгруппа,* $|H|=b$, $|W|=d$. *Тогда множество* $\Pi_{W,W}$ *является импримитивной подгруппой из* $S(H)$ *с системой импримитивности* $\{\beta+W|\beta\in H\}$. *Группа* $\Pi_{W,W}$ *подобна группе* $S_d \int S_{d^{-1}b}$.

В алгоритмах шифрования обычно используются операции и преобразования над векторным пространством $V_m(p)$, полем Галуа $GF(p^m)$ и кольцом вычетов $\mathbb{Z}_{p^m}$. Из следствия 2 непосредственно получаем описание множества $\Pi_{W,W}$ для этих случаев.

Утверждение 3. *Пусть* $(R,+)$ *— циклическая группа,* W *— произвольный нетривиальный подмодуль* R *-модуля* H, $|H|=b$, $|W|=d$. *Пусть также* X *— такое произвольное подмножество* H, *что* $|W|=|X|$. *Тогда*

$$\Pi_{W,X}=\begin{cases}\Pi_{W,W}g=(S_d \int S_{d^{-1}b})\,g, & \text{если } X \text{ — подмодуль } H,\\ \emptyset, & \text{иначе,}\end{cases}$$

где $g\in S(H)$, $g: W\to X$ *— произвольное линейное отображение.*

Напомним [5], что производной отображения s по направлению подпространства $L\le V_m$ называется отображение $(d_L s): V_m\to V_m$, заданное как $(d_L s):\beta\to\sum\limits_{\alpha\in L}{}_{\oplus}(\alpha\oplus\beta)^s$. Отметим, что производная отображения s по направлению подпространства также называется разностью высшего порядка [6]. Для произвольной подгруппы W абелевой группы H и произвольной подстановки $g\in S(H)$ введём обобщение $(ad_W g): H\to H$ разности высшего порядка d_L, полагая

$$(ad_W g):\beta\to\sum_{\alpha\in W}(\alpha+\beta)^g-|W|\beta^g.$$

При $(H,+)=(V_m,\oplus)$ получаем, что $ad_W=d_W$ для любого подпространства $W<V_m$.

Покажем, что множества $\Pi_{W,X}$ характеризуют некоторые свойства разностей высшего порядка.

Пусть $d_p(G)$ — p-ранг группы G, p — простое число, $p\ge 2$.

Утверждение 4.

1. *Пусть* H *— произвольная конечная абелева группа,* W,X *— такие её подгруппы одинаковой мощности, что* $\Pi_{W,X}\ne\emptyset$. *Тогда справедливо равенство* $\beta^{ad_W g}=\sum\limits_{\theta\in X}\theta$ *для любых* $\beta\in H$, $g\in\Pi_{W,X}$.

2. *Пусть выполнены условия пункта* 1 *и*

$$X \cong \mathbb{Z}_{p_1^{r_{11}}} \times \ldots \times \mathbb{Z}_{p_1^{r_{1d_1}}} \times \ldots \times \mathbb{Z}_{p_t^{r_{t1}}} \times \ldots \times \mathbb{Z}_{p_t^{r_{td_t}}},$$

где p_i — *простые числа,* $r_{ij} \in \mathbb{N}$, $p_i < p_{i+1}$, $r_{ij} \leq r_{ij+1}$, $d_i \in \mathbb{N}$, $i = \overline{1, t-1}$, $d_i \in \mathbb{N}$ $j = \overline{1, d_i - 1}$, $q = |X|$, e_{11} — *произвольный элемент группы* X *порядка* $p_1^{r_{11}}$. *Тогда*

$$\beta^{ad_W g} = \begin{cases} 2^{r_{11}-1} \left(\frac{q \cdot (2^{r_{11}}-1)}{2^{r_{11}}}\right) (\mathrm{mod} 2^{r_{11}}) e_{11}, & \text{если } d_2(X) = 1, \\ \vec{0}, & \text{иначе,} \end{cases}$$

Следствие 5. *Пусть* W, X — *нетривиальные подпространства* V_m, $|X| = |W|$, β — *произвольный вектор из* V_m, $s \in \Pi_{W,X}$. *Тогда*

$$\beta^{d_W s} = \begin{cases} \vec{0}, & \text{если } \dim W > 2, \\ \gamma = \vec{0}^s \oplus \alpha^s, & \text{если } \dim W = 2. \end{cases}$$

Список литературы

1. Evertse J. H. Linear structures in block ciphers // Eurocript'87. — Springer-Verlag, 1987.

2. Chaum D., Evertse J. H. Cryptanalysis of DES with a reduced number of rounds sequences of linear factors in block ciphers // Crypto'85. — Springer-Verlag, 1985.

3. Пудовкина М. А. Линейные структуры групп подстановок над конечным модулем // Прикладная дискретная математика. — 2008. — Т. 1. — С. 25–28.

4. Алексейчук А. Н., Скрынник Е. В. Классы отображений с тривиальной линейной структурой над конечным полем // Рестрациія, зберігання і обробка даних. — 2008. — Т. 10. — № 3. — С. 80–88.

5. Логачев О. А., Сальников А. А., Ященко В. В. Булевы функции в теории кодирования и криптологии. — М.: МЦНМО, 2004.

6. Knudsen L. R. Truncated and Higher Order Differentials // LNCS (FSE'95). — 1995. — V. 1008. — P. 196–211.

О ВЕРХНЕЙ ОЦЕНКЕ АФФИННОГО РАНГА НОСИТЕЛЯ СПЕКТРА ПЛАТОВИДНОЙ ФУНКЦИИ

Ю. В. Таранников (Москва)

Булева функция от n переменных — это отображение из F_2^n в F_2. *Преобразованием Уолша* булевой функции f называется целочисленная функция над F_2^n, определяемая как $W_f(u) = \sum\limits_{x \in F_2^n} (-1)^{f(x)+<u,x>}$. Для каждого $u \in F_2^n$ значение $W_f(u)$ называется *коэффициентом Уолша.* Коэффициенты Уолша называются *спектральными коэффициентами,* а совокупность всех 2^n коэффициентов Уолша — *спектром* булевой функции. Множество S_f всех наборов u, таких что $W_f(u) \neq 0$, называется *носителем спектра* функции f.

Булева функция называется *платовидной,* если ее коэффициенты Уолша принимают ровно три возможных значения: 0 и $\pm 2^c$ для некоторого c. Платовидные функции представляют большой интерес для изучения бент-функций (например, потому, что при разложении бент-функции по переменной возникают две платовидные функции), а также потому, что многие криптографически важные функции являются платовидными (например, m-устойчивые функции с максимально возможной для них нелинейностью $2^{n-1} - 2^{m+1}$). Из равенства Парсеваля сразу следует, что мощность носителя спектра равна 4^{n-c}.

Пусть E — произвольное подмножество F_2^n. *Рангом* множества E называется называется размерность подпространства, порожденного E в F_2^n. *Аффинным рангом* множества E называется называется размерность наименьшего класса смежности в F_2^n, содержащего E. Ранг и аффинный ранг носителя спектра булевой функции будем обозначать через k и $\mathbf{k}$, соответственно. Легко убедиться, что $\mathbf{k} \in \{k, k-1\}$. В [1] указано, что изучение платовидных функций на F_2^n с носителем спектра мощности 4^h можно в некотором смысле свести к изучению платовидных функций с носителем спектра той же мощности 4^h, заданных на $F_2^{\mathbf{k}}$. Более того, если $\mathbf{k} > 2h$, то любую платовидную функцию f' на F_2^n с носителем мощности 4^h можно получить из некоторой функции f на $F_2^{\mathbf{k}}$ с носителем той же мощности 4^h, добавив $n - \mathbf{k}$ фиктивных переменных и выполнив некоторое линейное преобразование функции. Того же можно добиться и в случае, если $\mathbf{k} = 2h$ и $W_{f'}(0) \neq 0$ (в этом случае функция f будет бент-функцией). Если $\mathbf{k} = 2h$ и $W_{f'}(0) = 0$, то указанного линейного преобразования функции не существует, но можно использовать аф-

финное преобразование спектра, либо же взять функцию f от $\mathbf{k}+1$ переменной.

Класс функций, близкий к платовидным функциям, изучался в [2]. В [2], в частности, были фактически проклассифицированы платовидные функции с носителем спектра мощности 16 и аффинным рангом носителя спектра 4, 5 и 6.

Очевидно, что если $|S_f| = 4^h$, то $\mathbf{k} \geq 2h$. В работе автора [1] для $h = 2$ было доказано, что аффинный ранг носителя спектра любой платовидной функции с носителем спектра мощности 16 равен 4, 5 или 6. Также в [1] для любого натурального h были построены платовидные функции с носителем спектра мощности 4^h (мощность обязана иметь такой вид), аффинный ранг носителя спектра которых принимает все возможные целые значения от $2h$ до $2^{h+1} - 2$. Тривиальной верхней оценкой мощности аффинного ранга носителя спектра платовидной функции является $\mathbf{k} \leq 4^h - 1$. В [1] была доказана несколько лучшая оценка $\mathbf{k} \leq 2^{2h-1} - 2^{h-1} + h$.

В настоящей работе получена верхняя асимптотическая оценка для величины $\mathbf{k}$.

Теорема. *Для аффинного ранга* $\mathbf{k}$ *носителя спектра мощности* 4^h *платовидных булевых функций при* $h \to \infty$ *имеет место асимптотическое неравенство*

$$\mathbf{k} \leq h \cdot 2^h (1 + \mathrm{o}(1)).$$

Кратко изложим основную идею доказательства теоремы. Из теоремы Титсворта следует, что для любого ненулевого $s \in F_2^n$ выполнено $\sum\limits_{x \in F_2^n} W_f(x) W_f(x+s) = 0$. На основании этого строится семейство подмножеств носителя спектра, причем наборы, входящие в каждое из подмножеств образуют линейно зависимую комбинацию. Кроме того, совокупность наборов каждого из подмножеств имеет дополнительное свойство, связанное с распределением знаков коэффициентов Уолша. Каждому из подмножеств семейства ставится в соответствие его характеристический двоичный набор длины 4^h. Рассматривается линейный код C над F_2^m, $m = 4^h$, порожденный совокупностью этих характеристических наборов. Для кода C с использованием указанных выше дополнительных свойств и верхней оценки его радиуса покрытия получается нижняя оценка его мощности, и, соответственно, верхняя оценка его коразмерности. Поскольку код C фактически соответствует множеству линейных зависимостей наборов из носителя спектра, верхняя оценка коразмерности C дает верхнюю оценку аффинного ранга носителя спектра.

Отметим, что имеющийся после настоящей работы разрыв между верхней и нижней оценками для $\mathbf{k}$ сходен с разрывом между оценками максимально возможного числа нелинейных переменных у корреляционно-иммунных функций высокого порядка [3].

Работа выполнена при поддержке грантов РФФИ 10–01–00475 и 08–01–00863, а также программы государственной поддержки ведущих научных школ НШ-4437.2010.1.

Список литературы

1. Тарannиков Ю. В. О значениях аффинного ранга носителя спектра платовидной функции // Дискретная математика. — 2006. — Т. 18, вып. 3. — С. 120–137.

2. Carlet C., Charpin P. Cubic Boolean functions with highest resiliency // IEEE Transactions on Information Theory. — February, 2005. — V. 51, № 2. — P. 562–571.

3. Тарannиков Ю. В. О корреляционно-иммунных и устойчивых булевых функциях // Математические вопросы кибернетики. Вып. 11. — М.: Физматлит, 2002. — С. 91–148.

ПОЛИНОМИАЛЬНОЕ ПРЕДСТАВЛЕНИЕ МНОЖЕСТВ, ГРАФОВ И СТРОК

В. Е. Федюкович (Киев)

В этом докладе предложен краткий обзор результатов, полученных путём решения задач о полиномах, эквивалентных некоторым задачам о множествах, графах и строках.

Полиномиальное представление множества элементов конечного поля было предложено [1] для задачи вычисления разности двух множеств, находящихся в распоряжении участников протокола (set reconciliation). Пусть $S = \{s_j\}$ — некоторое множество классов вычетов $\mathbb{Z}_q$ для некоторого простого q.

Определение 1. Характеристическим полиномом множества S называют $f(x, S) = \prod_{s_j \in S}(x - s_j)$

Определение 2. Задачей согласования множеств S_A и S_B, находящихся в распоряжении участников протокола A и B, называют вычисление $S_A \setminus S_B$ и $S_B \setminus S_A$ для последующего обмена недостающими элементами множеств.

Рассматривалась также задача [2] проверки одним из участников протокола утверждения о множествах, находящихся в распоряжении второго участника, причём основным условием такой проверки является предоставление проверяющей стороне только информации о справедливости проверяемого условия. Иными словами, проверяющая сторона не получает какой-либо полезной информации о множествах, а также не может убедить любую третью сторону в справедливости проверенного утверждения, в том числе предоставив всю информацию, полученную от доказывающей стороны в процессе такой проверки. Рассматривалось утверждение о верхней границе мощности разности множеств, так что проверяющая сторона получает информацию о множествах только в виде экземпляров привязки к элементам каждого из множеств.

Определение 3. Схемой привязки (commitment scheme) называют тройку алгоритмов инициализации параметров, создания и раскрытия экземпляра привязки, такую, что выполняются свойства полноты, связывания и скрытия. Схема имеет свойство полноты, если передающая сторона всегда успешно раскрывает экземпляр привязки, полученный ранее из некоторого значения. Схема имеет свойство связывания (binding), если имеется только ничтожная вероятность для любого алгоритма передающей стороны найти альтернативное значение, позволяющее успешно раскрыть любой экземпляр привязки. Схема имеет свойство скрытия (hiding), если имеется только ничтожное преимущество любого алгоритма соперника определить, какое из двух возможных, выбранных ранее соперником значений использовалось для создания экземпляра привязки.

Определение 4. Интерактивной системой аргумента (протоколом) для некоторого Булевого утверждения $R(x, w)$ называют интерактивную пару машин Тьюринга со словом x на ленте общего входа и с решением (witness) w на ленте дополнительного входа машины Доказывающего, такую что машина Проверяющего всегда принимает решение да/нет за полиномиально время и выполняются свойства полноты и корректности. Протокол имеет свойство полноты (completeness), если честный (honest) Проверяющий всегда принимает положительное решение для честного Доказывающего, а также входного слова и решения, таких что $R(x, w) = True$. Протокол имеет свойство корректности (soundness), если имеется только ничтожная вероятность для честного Проверяющего принять положительное решение для произвольного (any) Доказывающего, а также входного слова и решения, таких что $R(x, w) = False$.

Некоторые протоколы также имеют свойство нулевого разглашения [3] которое часто рассматривают как одно из основных по-

нятий современной криптографии. Значительный интерес представляет также метод Фиат—Шамира [4] преобразования протокола в схему электронной подписи, получивший название модели random oracle. Некоторые протоколы были реализованы [5,6] в виде серийно выпускаемых микросхем TPM и рассматриваются как перспективный способ защиты персональных данных.

Теорема 1. *Представление множества элементов конечного поля в виде характеристического полинома является уникальным.*

Рассматривалась также задача [7] о наличии K копий строки-шаблона в строке-тексте, с предоставлением проверяющей стороне информации о строках и смещениях шаблона в тексте только в виде экземпляров привязки схемы Damgard—Fujisaki [8] Пусть (c_j, i_j) — значение и позиция j-того символа строки, представленные в виде элементов кольца вычетов $\pmod N$ для некоторого составного N, факторизация которого неизвестна доказывающей стороне. Будем рассматривать строку как множество пар значение-позиция.

Определение 5. Характеристическим полиномом строки T будем называть $F(x, y, T) = \prod_{(c_j, i_j) \in T} (1 + xc_j + yi_j)$

Рассматривалась также классическая задача распознавания языка ориентированные гамильтоновы графы [9] Пусть Γ — ориентированный граф, заданный множеством вершин $\mathbb{V}(\Gamma)$ и множеством дуг $\mathbb{E}(\Gamma)$, с меткам вершин $a_v \in \mathbb{Z}_q$, $v \in \mathbb{V}(\Gamma)$.

Определение 6. Характеристическим полиномом орграфа Γ будем называть $F(x, y, \Gamma) = \prod_{\overrightarrow{H_j T_j} \in \mathbb{E}(\Gamma)} (1 + xa_{H_j} + ya_{T_j})$

Полиномиальное представление множеств, строк и графов может позволить формулировать эквивалентные задачи о полиномах и получать их решения.

Список литературы

1. Minsky Y., Trachtenberg A., Zippel R. Set reconciliation with nearly optimal communication complexity // International Symposium on Information Theory. — 2001. — P. 232.

2. Федюкович В. Е. Изменчивые ключи подписи // Безопасность информации в информационно-телекоммуникационных системах. — 2007.

3. Варновский Н. П. Типы нулевого разглашения // XI Международная школа-семинар "Синтез и сложность управляющих систем" (Нижний Новгород, 2000 г.). — М.: Изд-во ЦПИ при мех-мат ф-те МГУ, 2001. — С. 22-38.

4. Fiat A., Shamir A. How to prove yourself: Practical solutions to identification and signature problems // CRYPTO. — 1986. — P. 186–194.

5. Brickell E., Camenisch J., Chen L. Direct Anonymous Attestation // Cryptology ePrint Archive, Report 2004/205. — 2004.

6. Fedyukovych V. A strategy for any DAA Issuer and an additional verification by a Host // Cryptology ePrint Archive, Report 2008/277. — 2008.

7. Федюкович В. Е., Шарапов В. Г. Протокол демонстрации K-кратного вхождения строки // Информационные технологии и системы (ИТиС'08). — 2008. — С. 459–466.

8. Damgård I., Fujisaki E. A statistically-hiding integer commitment scheme based on groups with hidden order // ASIACRYPT. — 2002. — P. 125–142.

9. Fedyukovych V. An argument for Hamiltonicity // Cryptology ePrint Archive, Report 2008/363. — 2008.

ПОСТРОЕНИЕ 4-КОРРЕЛЯЦИОННО-ИММУННЫХ БУЛЕВЫХ ФУНКЦИЙ ОТ 9 ПЕРЕМЕННЫХ С НЕЛИНЕЙНОСТЬЮ 240

А. В. Халявин (Москва)

Одной из движущих задач теории булевых функций является задача построения булевых функций с экстремальными криптографическими характеристиками. В этой статье будет рассматриваться нелинейность и корреляционно-иммунность. *Нелинейностью* булевой функции называют минимальное расстояние до линейной булевой функции. Булеву функцию называют *корреляционно-иммунной* порядка m, если при подстановке констант вместо любых m аргументов доля единичных значений функции не изменяется. Эти характеристики хорошо выражаются на языке *коэффициентов Уолша*

$$W_f(u) = \sum_x (-1)^{(x,u)+f(x)}$$

булевой функции f.

Свойство корреляционно-иммунности порядка m равносильно выполнению равенства $W_f(u) = 0$ для наборов u с весом $1 \le wt(u) \le m$, а для нелинейности верна формула $nl(f) = 2^{n-1} - \frac{1}{2}\max_u |W_f(u)|$, где n — число аргументов у булевой функции (см. [1]). Кроме того, для любой булевой функции из *тождества Саркара* следует, что сумма коэффициентов Уолша по любому подкубу размерности

$k < n$ делится на 2^{k+1}. Исходя из этих фактов в [1,2] доказана оценка $nl(f) \leq 2^{n-1} - 2^m$ на нелинейность корреляционно-иммунной функции порядка m. Отсюда естественно возникает вопрос когда это неравенство является точным. Первым случаем, когда ответ на этот вопрос был не известен является $n = 9,\ m = 4$. Мы покажем, что такие функции с нелинейностью $nl(f) = 2^8 - 2^4 = 240$ существуют и опишем метод их поиска.

Использование свойств делимости позволяет многое сказать о коэффициентах Уолша функций с нужными нам свойствами. Оказывается, что ненулевые коэффициенты Уолша располагаются на наборах u с весами 0, 5, 6, 7 и 8 и равняются ± 32. Таким образом, остается подобрать знаки у коэффициентов Уолша. Кроме того, свойства делимости позволяют однозначно восстановить коэффициенты Уолша, зная их на слоях с весами 0 и 5. Действительно, для каждого из остальных коэффициентов можно вычислить сумму по всем меньшим наборам. Поскольку сумма должна делится по крайней мере на 2^{6+1}, то выбор знака у коэффициента определяется однозначно.

Заметим, что после повторного преобразования Уолша по *формуле обращения* должна получится целочисленная функция $2^n(-1)^{f(x)}$. Для удобства, можно поделить все коэффициенты Уолша на 32 и потребовать, чтобы после применения к ним преобразования Уолша получилась функция со значениями $\pm 2^9/32 = \pm 16$. Последовательность коэффициентов Уолша будем обозначать W, а ее преобразование Уолша — F, где $F(x) = 16 \cdot (-1)^{f(x)}$.

Далее разобъем коэффициенты Уолша на 4 части в зависимости от значений их битов с номерами 8 и 9. Обозначим их W_{00}, W_{01}, W_{10}, W_{11}. А их преобразования Уолша — F_{00}, F_{01}, F_{10}, F_{11}. Тогда выполнены равенства $F(x,i,j) = \sum_{a,b} F_{ab}(x)(-1)^{a\cdot i + b\cdot j}$ и $F_{ab}(x) = \frac{1}{4}\sum_{i,j} F(x,i,j)(-1)^{a\cdot i + b\cdot j}$. Откуда следует, что $F_{ab}(x)$ может принимать лишь значения 0, ± 8, ± 16. Кроме того, множество значений $F_{ab}(x)$ при фиксированном x состоит либо из ± 16 и трех нулей, либо из четырех чисел ± 8 среди которых нечетное число положительных и отрицательных.

Для начала вычислим какие значения может принимать часть W_{00}. Заметим, что наше множество функций обладает группой симметрий. Во-первых, можно обратить все коэффициенты Уолша (это соотвествует переходу от функции к ее отрицанию). Во-вторых, можно обратить все коэффициенты с i-м единичным битом (это соотвествует сдвигу функции вдоль i-го аргумента). В-третьих, можно переставлять аргументы у W (это соотвествует перестановке аргументов у f). В-четвертых, можно применить следующее линейное

преобразование к аргументам функции

$$W'(u_1, \ldots, u_9) = W(u_1 \oplus u_i, u_2 \oplus u_i, \ldots, u_i, \ldots, u_9 \oplus u_i).$$

Это преобразование переводит векторы веса $1, \ldots, 4$ в вектора веса $1, \ldots, 4$, а значит сохраняет свойство корреляционно-иммуности порядка 4. Значения коэффициентов Уолша не изменяются, а значит нелинейность сохраняется. Кроме того, как известно, невырожденные линейные преобразования коэффициентов Уолша соотвествуют невырожденным линейным преобразованиям исходной функции. Как показывают компьютерные рассчеты, использование всех этих симметрий позволяет свести все подходящие (у которых F_{00} принимает значения 0, ± 8, ± 16) значения части W_{00} к 5 случаям.

Для каждого из этих случаев рассмотрим какие значения может принимать часть W_{01}. В ней есть $\binom{7}{4} = 35$ наборов веса (с учетом 8 и 9 бита) 5. Используя возможность обратить все коэффициенты с 9 битом, можно зафиксировать один из них. Далее остается перебрать 2^{34} вариантов. Для каждого из них с помощью свойств делимости можно восстановить знаки всех остальных коэффициентов в части W_{01}, а затем проверить, что F_{01} принимает значения 0, ± 8, ± 16 и $|F_{01}(x)| + |F_{00}(x)| \leq 16$. Компьютерные вычисления показывают, что для каждого из 5 случаев есть 10–16 миллионов подходящих частей W_{01}. Наконец, варианты для W_{10} в точности совпадают с вариантами для W_{01} в силу симметрии.

Далее для одного из случаев выбирались случайные пары вариантов W_{01} и W_{10}. Если для какого либо x оказывалось, что среди $F_{00}(x)$, $F_{01}(x)$ и $F_{10}(x)$ есть более одного значения ± 16, то эта пара отбрасывалась. Если таких x не нашлось, то мы можем определить значения $F_{11}(x)$ во всех случаях кроме случая $F_{00}(x) = F_{01}(x) = F_{10}(x) = 0$, $F_{11}(x) = \pm 16$. Тогда каждое известное значение $F_{11}(x)$ дает нам линейное уравнение на ненулевые коэффициенты Уолша в $W_{11}(x)$. Остается решить эту систему, подставляя в свободные переменные ± 1 (для определенности системы как правило не хватает 5–7 уравнений). Все решения в которых ненулевые коэффициенты Уолша получаются целыми и равными ± 1 дают искомые функции. Решения находятся примерно для одной из $5 \cdot 10^5$ пар.

Работа выполнена при финансовой поддержке РФФИ (проект 08–01–00863), программы поддержки ведущих научных школ РФ (проект НШ–4437.2010.1) и программы фундаментальных исследований ОМН РАН «Алгебраические и комбинаторные методы математической кибернетики и информационные системы нового поколения».

Список литературы

1. Логачев О. А., Сальников А. А., Ященко В. В. Булевы функции в теории кодирования и криптографии. — М.: МЦНМО, 2004.

2. Тарannиков Ю. В. О корреляционно-иммунных и устойчивых булевых функциях // Математические вопросы кибернетики. Вып. 11. — М.: Физматлит, 2002. — С. 99–148.

О РАЗМЕРНОСТИ q-ИЧНЫХ ПРИМИТИВНЫХ БЧХ-КОДОВ

А. В. Чашкин (Москва)

В [1] Манн показал, что число информационных символов примитивного q-ичного БЧХ кода длины $n = q^m - 1$ с заданным конструктивным расстоянием вида $d = q^{m-l} - 1$ при достаточно большом n совпадает с ближайшим целым к y_0^l, где y_0 — максимальный положительный корень многочлена $f(y) = y^{l+1} - qy^l + q - 1$. Ниже приводится простая процедура вычисления y_0, которая для расстояний вида $d = q^{m-l} - 1$ позволяет усилить оценку Берлекемпа [2] скорости примитивных БЧХ-кодов.

Введем функции $\varphi_1(k, l)$ и $\varphi_2(k, l)$, положив

$$\varphi_1(1, l) = \Big(1 - \frac{q-1}{q^{l+1}}\Big)^{-l}, \qquad \varphi_1(k, l) = \Big(1 - \frac{q-1}{q^{l+1}} \cdot \varphi_1(k-1, l)\Big)^{-l},$$

$$\varphi_2(1, l) = \Big(1 - \frac{q-1}{q^{l}}\Big)^{-l}, \qquad \varphi_2(k, l) = \Big(1 - \frac{q-1}{q^{l+1}} \cdot \varphi_2(k-1, l)\Big)^{-l}.$$

Индукцией по k нетрудно показать, что функция $\varphi_1(k, l)$ возрастает по k, а функция $\varphi_2(k, l)$ убывает по k при любом $l \geq 2$. Так как

$$\frac{q-1}{q^{l+1}}\Big(1 - \frac{q-1}{q^{l+1}}\Big)^{-l} > \frac{q-1}{q^{l+1}},$$

то справедливо неравенство

$$\varphi_1(2, l) = \Big(1 - \frac{q-1}{q^{l+1}}\Big(1 - \frac{q-1}{q^{l+1}}\Big)^{-l}\Big)^{-l} > \varphi_1(1, l) = \Big(1 - \frac{q-1}{q^{l+1}}\Big)^{-l},$$

которое используем как основание индукции для доказательства возрастания функции $\varphi_1(k,l)$ по k. Допустим, что $\varphi_1(k,l) > \varphi_1(k-1,l)$, тогда

$$\varphi_1(k+1,l) = \Big(1-\frac{q-1}{q^{l+1}}\cdot\varphi_1(k,l)\Big)^{-l} > \varphi_1(k,l) = \Big(1-\frac{q-1}{q^{l+1}}\cdot\varphi_1(k-1,l)\Big)^{-l}.$$

Таким образом $\varphi_1(k,l)$ возрастает по k. Аналогичным образом доказывается убывание по k функции $\varphi_2(k,l)$.

Положим

$$\psi_1(k,l) = q\Big(1-\frac{q-1}{q^{l+1}}\cdot\varphi_1(k,l)\Big), \qquad \psi_2(k,l) = q\Big(1-\frac{q-1}{q^{l+1}}\cdot\varphi_2(k,l)\Big).$$

Из монотонности функций $\varphi_i(k,l)$ следует, что функция $\psi_1(k,l)$ убывает по k, а функция $\psi_2(k,l)$ возрастает по k. Так как $0 < \psi_i(k,l) < q$, то, очевидно, существуют пределы $\lim_{k\to\infty}\psi_1(k,l) = \psi_1(l)$ и $\lim_{k\to\infty}\psi_2(k,l) = \psi_2(l)$.

Покажем, что

$$f(\psi_2(k,l)) < f(y_0) = 0 < f(\psi_1(k,l)).$$

Сначала докажем правое неравенство. Для этого вычислим $f(\psi_1(k,l))$ и воспользуемся возрастанием $\varphi_1(k,l)$ по k. Нетрудно видеть, что

$$f(\psi_1(k,l)) = \Big(q\Big(1-\frac{q-1}{q^{l+1}}\varphi_1(k,l)\Big)\Big)^{l+1} - q\Big(q\Big(1-\frac{q-1}{q^{l+1}}\varphi_1(k,l)\Big)\Big)^{l} + q - 1$$

$$= q^{l+1}\Big(1-\frac{q-1}{q^{l+1}}\varphi_1(k,l)\Big)^{l}\Big(1-\frac{q-1}{q^{l+1}}\varphi_1(k,l)-1\Big) + q - 1$$

$$= -\Big(1-\frac{q-1}{q^{l+1}}\varphi_1(k,l)\Big)^{l}(q-1)\varphi_1(k,l) + q - 1 = -\frac{(q-1)\varphi_1(k,l)}{\varphi_1(k+1,l)} + q - 1 > 0.$$

Вычисляя $f(\psi_2(k,l))$ и используя убывание $\varphi_2(k,l)$ по k, видим, что

$$f(\psi_2(k,l)) = \Big(q\Big(1-\frac{q-1}{q^{l+1}}\cdot\varphi_2(k,l)\Big)\Big)^{l+1} - q\Big(q\Big(1-\frac{q-1}{q^{l+1}}\cdot\varphi_2(k,2)\Big)\Big)^{l} + q - 1$$

$$= q^{l+1}\Big(1-\frac{q-1}{q^{l+1}}\varphi_2(k,l)\Big)^{l}\Big(1-\frac{q-1}{q^{l+1}}\varphi_2(k,l)-1\Big) + q - 1$$

$$= -\left(1-\frac{q-1}{q^{l+1}}\varphi_2(k,l)\right)^l (q-1)\varphi_2(k,l)+q-1 = -\frac{(q-1)\varphi_2(k,l)}{\varphi_2(k+1,l)}+q-1 < 0.$$

Неравенства для $f(\psi_1(k,l))$ и $f(\psi_2(k,l))$ доказаны. Из этих неравенств и возрастания $f(y)$ в окрестности y_0 следует, что

$$\psi_2(k,l) \le \psi_2(l) \le y_0 \le \psi_1(l) \le \psi_1(k',l)$$

при любых k и k'. Далее нетрудно видеть, что

$$f(\psi_1(k,l)) - f(\psi_2(k,l)) = (q-1)\left(\frac{\varphi_2(k,l)}{\varphi_2(k+1,l)} - \frac{\varphi_1(k,l)}{\varphi_1(k+1,l)}\right).$$

Так как с ростом k отношения $\frac{\varphi_1(k,l)}{\varphi_1(k+1,l)}$ и $\frac{\varphi_2(k,l)}{\varphi_2(k+1,l)}$ стремятся к единице, то очевидно, что разность $f(\psi_1(k,l))-f(\psi_2(k,l))$ стремится к нулю, а следовательно, к нулю стремится и разность $\psi_1(k,l)-\psi_2(k,l)$. Поэтому $\psi(l) = \psi_1(l) = \psi_2(l)$. Из определения величин $\psi_1(k,l)$ и $\psi_2(k,l)$ следует, что с ростом k стремится к нулю и разность $\varphi_2(k,l)-\varphi_1(k,l)$, а так как $\varphi_i(k,l)$ монотонны по k, то

$$\lim_{k\to\infty} \varphi_1(k,l) = \lim_{k\to\infty} \varphi_2(k,l) = \varphi(l),$$

и, следовательно, величина

$$\psi(l) = q\left(1 - \frac{q-1}{q^{l+1}}\varphi(l)\right)$$

является искомым корнем y_0 многочлена $f(y)$.

Работа выполнена при финансовой поддержке РФФИ (проект 08–01–00863) и программы поддержки ведущих научных школ РФ (проект НШ–4437.2010.1).

Список литературы

1. Манн Г. Б. О числе информационных символов в кодах Боуза—Чоудхури // Кибернетический сборник. Вып. 8. — М.: Мир, 1966. С. 33–41.

2. Berlekamp E. Long primitive binary BCH codes have distance $d \sim 2n\ln R^{-1}/\log n$ // IEEE Transactions on Information Theory. — May 1972. — V. 18, № 3. — P. 415–426.

СПИСОК ПЛЕНАРНЫХ ДОКЛАДОВ, ПРОЧИТАННЫХ НА СЕМИНАРЕ

В. Б. Алексеев (Москва) *О работах Сергея Всеволодовича Яблонского (к 85-летию со дня рождения)*

М. П. Минеев, В. Н. Чубариков (Москва) *Некоторые арифметические вопросы криптографии*

А. Б. Угольников (Москва) *О некоторых задачах в области многозначных логик*

В. Б. Кудрявцев (Москва), И. С. Грунский, В. А. Козловский (Донецк) *Анализ и синтез абстрактных автоматов*

Д. Н. Бабин (Москва) *Классификация автоматных базисов Поста по разрешимости свойств полноты и A-полноты*

Ф. М. Аблаев (Казань) *Вычислительные возможности классических и квантовых ветвящихся программ*

В. А. Ватутин (Москва) *Ветвящиеся процессы, случайные деревья и случайные отображения*

Ф. И. Соловьева (Новосибирск) *Совершенные коды и смежные вопросы (обзор)*

Л. А. Шоломов (Москва) *Элементы теории недоопределенной информации*

В. А. Копытцев, В. Г. Михайлов (Москва) *Теорема пуассоновского типа для числа специальных решений системы случайных линейных уравнений над конечным полем*

В. К. Леонтьев (Москва) *О некоторых комбинаторных задачах*

В. С. Макаров (Москва) *Правильные многогранники и многогранники с правильными гранями в пространстве Лобачевского*

Ю. Н. Черемных (Москва) *Математические методы в анализе и прогнозировании экономических процессов*

Р. И. Подловченко (Москва) *О распознавании эквивалентности в алгебраических моделях программ*

В. Н. Шевченко (Нижний Новгород) *Триангуляции выпуклых многогранников и их f-векторы*

А. Ю. Чирков (Нижний Новгород) *Оценки числа крайних точек в задаче ЦЛП*

А. А. Ирматов (Москва) *Комбинаторно-топологические и вероятностные аспекты оценки числа пороговых функций*

В. В. Кочергин (Москва) *О задачах Д. Кнута и Р. Беллмана, их обобщениях и близких вопросах*

С О Д Е Р Ж А Н И Е

Пленарные доклады

Секция «Синтез, сложность и надежность управляющих систем»

Секция «Функциональные системы»

Секция
«Комбинаторный анализ и теория графов»

Подсекция «Комбинаторный анализ»

Подсекция «Теория графов»

Секция «Математическая теория интеллектуальных систем»

Секция «Дискретная геометрия»

Секция «Теория кодирования и смежные вопросы»